Шень, Александр

Алгоритмические варианты понятия энтропии

Москва
Российская государственная библиотека
diss.rsl.ru
2006

Шень, Александр

Алгоритмические варианты понятия энтропии [Электронный ресурс] : Дис. ... канд. физико-математические науки : 01.01.06. - М.: РГБ, 2006. - (Из фондов Российской государственной библиотеки)

Математическая логика, алгебра и теория чисел

Шень, Александр

Алгоритмические варианты понятия энтропии

Москва, 1984

Министерство высшего и среднего специального
образования СССР
Московский орденов Ленина, Октябрьской революции
и Трудового Красного Знамени государственный
университет имени М.В.Ломоносова

Механико-математический факультет

На правах рукописи

ШЕНЬ Александр

УДК 517.11

Алгоритмические варианты понятия энтропии

(01.01.06 - алгебра, теория чисел, математическая логика)

Диссертация
на соискание ученой степени кандидата
физико-математических наук

Научный руководитель:
доктор физико-математических наук
профессор УСПЕНСКИЙ В.А.

Москва, 1984 г.

П р е д и с л о в и е.

Вопросы, рассматриваемые в диссертации, относятся к алгоритмической теории вероятностей . Обзор содержания диссертации дан во введении. Цифры в квадратных скобках означают ссылки на приведенный в конце диссертации список литературы.

Автор благодарит своего учителя Владимира Андреевича Успенского за постоянное внимание и поддержку.

Введение.

В 1965 году А.Н.Колмогоров ввел понятие сложности, или энтропии[ж)], конечного объекта (см. [7], [8]). Говоря неформально, энтропия объекта есть количество двоичных знаков, необходимых для описания (задания, определения) этого объекта. Разумеется, это количество зависит от выбора способа описания; таким образом, каждому способу описания соответствует своя функция сложности. Открытие Колмогорова как раз и состояло в том, что при естественном определении понятия "способ описания" среди всех таких способов существует оптимальный - такой, при котором сложность объектов меньше, чем при любом другом (с точностью до ограниченного слагаемого). Если имеются два разных оптимальных способа описания, то соответствующие им сложности отличаются, очевидно, на ограниченное слагаемое. Таким образом, возможно дать не зависящее от выбора способа описания определение энтропии конечного объекта как его сложности при оптимальном способе описания. Введенную Колмогоровым энтропию мы будем называть простой колмогоровской энтропией.

Позднее были предложены другие варианты понятия энтропии конечного объекта - сложность (энтропия) разрешения (см. [5]), префиксная энтропия, монотонная энтропия (о двух последних см. [2]). Хотя эти понятия основаны на родственных идеях - все они тем или иным способом уточняют описанный выше замысел Колмогорова,- их формальные определения никак не были связаны друг с другом. Ниже предлагается некоторая общая схема, част-

ж) Мы предпочитаем термин "энтропия", чтобы избежать смешения со "сложностями вычисления" (временной, емкостной и т.п.)

ными случаями которой являются все перечисленные (а также некоторые другие) варианты определения понятия энтропии конечного объекта.

Эта схема использует понятие f_0 -пространства в смысле Ю.Л.Ершова [4] . Понятие f_0 -пространства является чрезвычайно удобным средством для определения вычислимости отображений, область определения которых состоит из объектов более сложной природы, чем натуральные числа (функций, последовательностей и т.д.). Поясним это понятие на следующем важном примере.

Пусть мы имеем отображение $\mathfrak{A}$, область определения которого состоит из (частичных) функций из $\mathbb{N}$ в $\mathbb{N}$. Пусть это отображение в каком-то смысле вычислимо. Естественно считать, что к любому моменту процесса вычисления значения $\mathfrak{A}$ на функции f используется не вся информация о f (ибо как может алгоритмический процесс успеть использовать бесконечно много информации об f ?!), а лишь конечное число равенств вида $f(a) = b$. Другими словами, значение отображения $\mathfrak{A}$ на функции f определяется значениями этого отображения на конечных частях f . Ясно также, что по мере увеличения использованной информации об f будет получаться все больше и больше информации о результате применения $\mathfrak{A}$ к f (если этот результат также является функцией, то будут становиться известными ее значения во все большем числе точек).

Эти соображения показывают, что при определении понятия вычислимости для функций из некоторого множества X в другое множество Y в множествах X и Y естественно выделять "конечные" элементы (в примере - функции с конечными областями определения) и вводить отношение "элемент a'

информативнее элемента a " (в примере - функция f' продолжает функцию f). Более формально, f_0 -пространством называется множество X , в котором введено отношение частичного порядка $x \leq x'$ (читаемое " x' информативнее x ", " x' продолжает x " или " x есть часть x' ") и выделено некоторое подмножество $X_0 \subset X$, элементы которого называются конечными, причем выполнены некоторые свойства (см. п. I.I). В нашем примере X есть множество всех (частичных) функций из $\mathbb{N}$ в $\mathbb{N}$ с указанными выше подмножеством конечных элементов и отношением "быть более информативным". Высказанные выше соображения можно теперь, с помощью понятия f_0 -пространства, сформулировать более точно: вычислимое отображение $\mathfrak{A}$ из f_0 -пространства X в f_0 -пространство Y должно быть монотонным (т.е. $X \leq X' \Rightarrow \mathfrak{A}(x) \leq \mathfrak{A}(x')$) и значение $\mathfrak{A}$ на x должно определяться значениями $\mathfrak{A}$ на конечных частях x , т.е. на тех $x_0 \in X_0$, для которых $x_0 \leq x$. См. об этом подробно в пп. I.4 и I.5.

Другая важная идея, которую использует описываемая схема определения энтропии - идея интерпретации операций логики высказываний (конъюнкции, дтзъюнкции, импликации) как операций не над утверждениями, а над задачами. Эта идея была предложена А.Н.Колмогоровым в [18] и уточнена впоследствии Ю.Т.Медведевым в [9] . Говоря неформально, задача определяется двумя множествами - множеством X "возможных решений" задачи и его подмножеством A - подмножеством "действительно решений". Например, задачу "перечислить все элементы множества $Q \subset \mathbb{N}$ " можно рассматривать как пару таких множеств: множеством возможных решений считается множество всех последовательностей натуральных чисел, а действительными ре-

шениями считаются те последовательности $n \mapsto x_n$, для которых $\{x_n \mid n \in \mathbb{N}\} = Q$. Можно сказать, что задача $\langle X, A \rangle$ есть задача "отыскания среди элементов X элемента, принадлежащего A".

Наш вариант уточнения понятия задачи отличается тем, что в нем используются f_0 -пространства в качестве множеств возможных решений и соответствующим образом определяются операции над задачами.

Опишем в общих чертах предлагаемую схему определения энтропии. Пусть имеются два f_0 - пространства - X и Y. Элементы первого мы будем считать описаниями (кодами), а элементы второго - описываемыми (кодируемыми) объектами. Пусть на множестве конечных объектов пространства X введена функция объема (сопоставляющая каждому конечному объекту некоторое число). Способами описания будем считать вычислимые (в смысле, описываемом в I.5) отображения $f: X \to Y$. Сложность задачи $\langle Y, A \rangle$ в пространстве Y при способе описания f определяется как минимальный среди объемов тех описаний $x \in X_0$, для которых $f(x) \in A$.
При некоторых условиях на пространство X (см. п. 2.3) среди всех способов описания существует оптимальный; сложность задачи $\langle Y, A \rangle$ при оптимальном способе описания мы и назовем энтропией этой задачи. Если X и Y выбраны из числа пространств $\mathbb{N}_\perp$ и Ω (пространства натуральных чисел и пространства последовательностей нулей и единиц, описание которых дано в I.2), возможны четыре варианта, изображенные в таблице:

пространство описываемых объектов / пространство описаний	$\mathbb{N}_\perp$	Ω
$\mathbb{N}_\perp$	K	KR
Ω	KP	KM

В ней указано, каким из упоминавшихся выше вариантов понятия энтропии соответствует возникающее при данных пространствах описываемых объектов и описаний понятие энтропии задачи:

K – простая колмогоровская энтропия, KR – энтропия (сложность) разрешения, KP – префиксная энтропия, KM – монотонная энтропия.

В работе исследуются свойства описанной схемы. Устанавливается ее связь с интуиционистской логикой высказываний. С точки зрения этой схемы исследуется также понятие априорной вероятности. Дадим теперь более подробный обзор содержания работы.

Глава I носит вспомогательный характер и содержит понятия и результаты, в основном не являющиеся новыми (см. [4]). Мы сочли нужным поместить здесь этот материал, т.к. изложение его в виде, используемом в последующих разделах, в литературе отсутствует. Эта глава посвящена понятию f_0 -пространства и связанным с ним конструкциям.

В п. I.I дается определение f_0 -пространства и вводится связанныя с ним терминология. Именно, f_0 -пространством называется тройка $\langle X, \leq, X_c \rangle$ (X – некоторое множество,

$\leq$ – частичный порядок на нем, X_0 – некоторое подмножество множества X), обладающая определенными свойствами (см. подробнее п. I.I). Элементы множества X называются объектами, отношение $x \leq x'$ читается " x' продолжает x" или " x есть часть x'", объекты, входящие в X_0 , называются конечными. Наименьший в смысле введенного порядка объект называется неопределенностью и обозначается $\perp$.

В п. I.2 строятся основные примеры f_0-пространств, существенные для дальнейшего. Среди них – уже упоминавшиеся пространства $\mathbb{N}_\perp$ (натуральных чисел) и Ω (последовательностей нулей и единиц).

В п. I.3 вводится понятие полного f_0-пространства и показывается, что всякое f_0-пространство можно рассматривать как часть полного. Это позволяет в дальнейшем ограничиться рассмотрением полных пространств. Доказываются свойства полных пространств, используемые далее.

В п. I.4 вводятся операции над f_0-пространствами. Именно, для любых двух пространств X и Y определяются пространства $X \times Y$ (произведение), $X + Y$ (сумма) и $C(X, Y)$ (пространство непрерывных функций из X в Y). Для определения непрерывности в f_0-пространствах вводится топология. Дается простой критерий непрерывности функции (лемма 4). Устанавливается, что непрерывную функцию можно задать, указав ее значения на конечных объектах. Устанавливаются естественные изоморфизмы

$$C(X, C(Y, Z)) \simeq C(X \times Y, Z)$$
$$C(X, Y \times Z) \simeq C(X, Y) \times C(X, Z)$$

Чтобы определить понятие вычислимого объекта, в f_0-пространстве нужно ввести дополнительную структуру, занумеровав

все конечные объекты этого пространства натуральными числами. Пространство, снабженное такой нумерацией, называется эффективным f_0 -пространством, если выполнены некоторые естественные требования; соответствующие определения даются в I.5. В этом же пункте показано, как ввести структуру эффективного пространства в $X \times Y$, $X + Y$, $C(X, Y)$ (если X и Y - эффективные пространства), а также в f_0 -пространствах, указанных в п. I.2.

В эффективных пространствах вводится понятие вычислимого объекта. Вычислимые объекты пространства $C(X,Y)$ естественно рассматривать как вычислимые отображения из X в Y. Они используются для определения относительной вычислимости: объект $y \in Y$ называется вычислимым относительно объекта $x \in X$, если существует вычислимый объект $f \in C(X, Y)$, для которого $f(x) = y$. В п. I.5 показывается, каким образом известные варианты понятия относительной вычислимости становятся частными случаями этой схемы. Устанавливается используемое в дальнейшем (при доказательстве утверждения о существовании оптимального способа описания) предложение о перечислимости множества всех вычислимых объектов (предложение I).

Наконец, в п. I.6 на рассмотренных пространствах вводится объем.

Этим завершается изложение необходимых сведений об эффективных полных f_0 -пространствах (называемых в дальнейшем для краткости просто пространствами).

В главе 2 определяется понятие задачи, среди всех задач выделяются разрешимые, которые и классифицируются по "трудности решения" с помощью понятия энтропии.

В п. 2.I дается определение понятия задачи. Именно, задачей называется пара $\langle X, A\rangle$, где X - пространство, а $A\subset X$. Среди задач выделяются монотонные (те, у которых любое продолжение решения является решением) и разрешимые (те, у которых среди решений есть вычислимые).

В п. 2.2 уточняется понятие способа описания объектов пространства Y с помощью объектов пространства X - такими способами считаются вычислимые объекты пространства $C(X,Y)$. Если на X задан объем ℓ и фиксирован способ описания $f\in C(X,Y)$, то можно определить сложность задачи $\langle Y, A\rangle$ при способе описания f как

$$\inf\{\ \ell(x)\ |\ x \text{ - конечный объект } X,\ f(x)\in A\}.$$

В п. 2.3 даны условия на пространство X , необходимые и достаточные для того, чтобы для любого пространства Y среди всех способов описания из $C(X,Y)$ существовал оптимальный. Пространства X с объемом ℓ , обладающие таким свойством, называются регулярными. Пусть X - регулярное пространство. Сложность задач в пространстве Y при оптимальном способе описания $f\in C(X,Y)$ мы называем энтропией (точнее, X -энтропией). Произвол в выборе оптимального способа описания влечет за собой то, что энтропия определена с точностью до ограниченного слагаемого. Энтропия задачи оказывается конечной в том и только том случае, когда эта задача разрешима (предложение 2)

В п. 2.4 приводятся примеры регулярных пространств с объемом ($\mathbb{N}_\perp$, Ω , Ξ). Каждому из них соответствует свой вид энтропии.

Их сравнению посвящен п. 2.5. Именно, там дается ответ на следующий вопрос. Пусть X_1 и X_2 - два регулярных пространства. В каком случае для любой задачи α выполнено

неравенство

$$(X_1\text{-энтропия } \alpha) \leq f(X_2\text{-энтропия } \alpha) \quad ?$$

(Более точную постановку вопроса, учитывающую то, что энтропия определена с точностью до ограниченного слагаемого, см. далее) Ответ на этот вопрос дается предложениями I и 2. С их помощью сравниваются пространства $\mathbb{N}_\perp$, Ω и Ξ.

В п. 2.6 сравниваются, напротив, энтропии задач в разных пространствах при одном и том же пространстве описаний.

Глава 3 посвящена связи между понятием задачи и интуиционистской логикой высказываний.

В п. 3.I определяются (в духе идей Колмогорова [18], развитых Медведевым [9]) логические операции над задачами (конъюнкция, дизъюнкция и импликация). Говоря неформально, возможными решениями задачи $\alpha \wedge \beta$ считаются пары $\langle$возможное решение задачи α, возможное решение задачи $\beta\rangle$, а решениями – те пары, оба члена которых действительно являются решениями соответствующих задач. Возможными решениями задачи $\alpha \vee \beta$ считаются все возможные решения задачи α, все возможные решения задачи β и объект $\perp$; решениями считаются решения любой из задач α и β. Возможными решениями задачи $\alpha \supset \beta$ считаются непрерывные (в этом главное отличие от [9]) функции, переводящие возможные решения задачи α в возможные решения задачи β; функция f будет считаться решением, если для любого решения x задачи α объект $f(x)$ будет решением задачи β. Ложь интерпретируется как задача, у которой множество решений пусто, а множество возможных решений одноэлементно.

В п. 3.2 рассматриваются энтропии задач $\alpha \wedge \beta$, $\alpha \vee \beta$ и $\alpha \supset \beta$. Выясняется, что энтропия задачи $\alpha \vee \beta$ определяется энтропиями задач α и β. Исследуются энтропии

задач $\alpha \wedge \beta$ ("энтропия пары") и $\alpha \supset \beta$ ("условная энтропия β при известном α ").

В п. 3.3 определяется интерпретация интуиционистской логики высказываний с помощью задач. Именно, пусть $\Phi(p_1, .., p_n)$ – формула логики высказываний, $\alpha_1 = \langle X_1, A_1 \rangle, \dots, \alpha_n = \langle X_n, A_n \rangle$ – задачи. Тогда в соответствии с описанной интерпретацией конъюнкции, дизъюнкции и импликации возникает задача $\Phi(\alpha_1, \dots, \alpha_n)$. Легко видеть, что множество возможных решений этой задачи зависит только от пространств X_i (но не от множеств A_i). Оказывается, что если Φ – выводимая в интуиционистской логике высказываний формула, то в этом пространстве найдется вычислимый объект x , являющийся решением задачи $\Phi(\alpha_1, \dots, \alpha_n)$ при любых $A_1, \dots, A_n$. (Это утверждение является аналогом известного результата Ю.Т.Медведева [9])

В п. 3.4 из этой теоремы выводится ряд неравенств для энтропии некоторых задач (предложение I и его следствия).

В п. 3.5 исследуется логика задач, то есть множество Q формул, общезначимых в описанном смысле. Как уже говорилось, множество H выводимых в интуиционистском исчислении высказываний формул является подмножеством Q , которое в свою очередь является подмножеством множества C пропозициональных тавтологий. Устанавливается, что оба включения $H \subset Q$ и $Q \subset C$ – строгие.

Глава 4 посвящена дальнейшему исследованию введенного понятия энтропии. В п. 4.I показано, каким образом различные известные варианты понятия энтропии (простая колмогоровская энтропия [7] , условная колмогоровская энтропия [7] , энтропия (сложность) разрешения [5] , префиксная энтропия [2] , монотонная энтропия [2] , номер частично рекурсивной функции

в оптимальной нумерации [20, 21]) включаются в описанную схему.

В п. 4.2 показывается, каким образом многочисленные неравенства, связывающие различные виды энтропии, могут быть получены как следствия доказанных в главе 2 общих теорем. Доказывается, что некоторые оценки, связывающие четыре варианта энтропии из приведенной выше таблицы (K , KR, KP , KM) нельзя улучшить.

В п. 4.3 с точки зрения нашей схемы исследуется понятие априорной вероятности (см. [2],[5]). Именно, для каждой задачи $\langle X, A\rangle$ и для каждого способа описания $f \in C(\Omega, X)$ объектов пространства X с помощью двоичных последовательностей определяется число $P_f(\langle X,A\rangle)$ - вероятность того, что случайно взятая из Ω последовательность будет описанием решения задачи $\langle X, A\rangle$. Среди всех способов описания существует оптимальный - тот, при котором P_f максимальна (с точностью до ограниченного множителя). Функция P_f при оптимальном f и называется априорной вероятностью. В пространствах $\mathbb{N}_\perp$ и Ω она совпадает с так называемой максимальной перечислимой мерой (см. [2], [5]). Мы доказываем, что аналогичное свойство выполнено для всех пространств, в которых множество конечных объектов является деревом. Это условие существенно: в п. 4.3 приводится пример, показывающий, что в пространстве Ξ априорная вероятность не является максимальной перечислимой мерой.

Глава I. Понятие f_0 -пространства и его свойства.

В этой главе определяется понятие f_0 -пространства, строятся примеры f_0 -пространств, существенные для дальнейшего, и описываются простейшие конструкции, позволяющие получать новые f_0 -пространства из уже имеющихся. В ней также вводятся понятия полного f_0-пространства, эффективного f_0-пространства, вычислимого объекта и доказываются связанные с этими понятиями утверждения, необходимые в дальнейшем.

Последний пункт главы определяет понятие объема на f_0 -пространстве, играющее в дальнейшем важную роль.

1.1. Определение f_0-пространства.

Пусть заданы множество X с частичным порядком $\leq$ на нем и подмножество $X_0 \subset X$. Тройка $\langle X, X_0, \leq \rangle$ называется f_0 -пространством, если выполнены следующие свойства:

(1) В X существует наименьший (в смысле частичного порядка на X) элемент. Этот элемент (обозначаемый $\perp$) принадлежит X_0 .

(2) Если $x, y \in X_0$, $z \in X$, $x \leq z$, $y \leq z$, то x и y имеют в X точную верхнюю грань $\sup(x,y)$, лежащую в X_0 : для всех $t \in X$ утверждения $(x \leq t) \& (y \leq t)$ и $\sup(x,y) \leq t$ равносильны.

(3) Если $x, y \in X$ и $x \nleq y$, то существует $x_0 \in X_0$, для которого $x_0 \leq x$ и $x_0 \nleq y$.

Пусть $\langle X, X_0, \leq \rangle$ - f_0-пространство; элементы множества X мы будем называть объектами этого пространства, запись $x \leq y$ читать "объект y продолжает объект x " или "объект x есть часть объекта y " ; объекты, входящие в X_0 , будем называть конечными. Объект $\perp$ мы будем называть неопределенностью. Объекты x и y , для которых существует такой объект z , что $x \leq z$ и $y \leq z$, мы будем называть совместными.

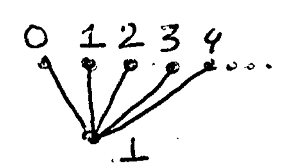
I.2. Основные примеры f_0-пространств.

В этом пункте мы построим некоторые f_0-пространства, которые будут полезны нам в дальнейшем.

I.2.I. Простейшее f_0-пространство состоит из единственного элемента $\perp$.

I.2.2. Пространство $X = \{\perp, *\}$, $X_0 = X$, порядок таков: $\perp \le *$.

I.2.3. Пространство натуральных чисел, дополненных объектом $\perp$; в нем



$X = \{\perp, 0, 1, 2, \ldots\}$,

$X_0 = X$, порядок таков: $\perp \le n$ для всех $n = 0, I, 2, \ldots$ и других неравенств нет. Это пространство мы будем обозначать $\mathbb{N}_\perp$.

I.2.4. Пространство конечных и бесконечных последовательностей 0 и I. В этом пространстве объекты – конечные и бесконечные последовательности 0 и I, $x \le y$, если последовательность x является началом последовательности y, конечными объектами являются конечные последовательности. Это пространство мы будем обозначать Ω. В нем обозначение $\perp$ получает пустое слово.

I.2.5. Пространство подмножеств $\mathbb{N}$. Объектами являются подмножества $\mathbb{N}$, $x \le y$ означает $x \subset y$, конечные объекты суть конечные множества. Это пространство мы будем обозначать $2^{\mathbb{N}}$.

I.2.6. Пространство частичных функций натурального аргумента со значениями 0 и I. Его объектами являются частичные функции из $\mathbb{N}$ в $\{0, 1\}$, $x \le y \Leftrightarrow y$ есть продолжение x, конечными объектами являются функции, области определения которых – конечные множества. Это пространство мы обозначим Ξ.

I.2.7. Заменив в примерах I.2.4 и I.2.6 множество

$\{0, 1\}$ на множество $\mathbb{N}$ (т. е. рассматривая последовательности натуральных чисел и функции из $\mathbb{N}$ в $\mathbb{N}$), мы приходим к пространству $\mathcal{S}$ конечных и бесконечных последовательностей натуральных чисел и к пространству $\mathbb{F}$ частичных функций из $\mathbb{N}$ в $\mathbb{N}$.

I.2.8. Любую верхнюю полурешетку с наименьшим элементом (частично упорядоченное множество, в котором любые два элемента имеют точную верхнюю грань и есть наименьший элемент) можно превратить в f_0-пространство, объявив конечными все объекты.

I.3. Полные f_0-пространства.

В этом пункте мы изучим простейшие свойства f_0-пространств; в частности, будет введено понятие полного f_0-пространства.

Пусть дано f_0-пространство $\langle X, X_0, \leq \rangle$ Назовем множество $I \subset X_0$ идеалом, если выполнены следующие свойства:

(а) I непусто;

(б) если $y, z \in X_0$, $y \leq z$, $z \in I$, то $y \in I$;

(в) если $y, z \in I$, то y и z совместны и $\sup(y, z) \in I$.

Сопоставим каждому объекту $x \in X$ множество I_x всех его конечных частей:

$$I_x = \{ y \in X_0 \mid y \leq x \}$$

Справедлива следующая простая

Лемма I. Множество I_x является идеалом. ▨

Таким образом, каждому элементу x сопоставлен некоторый идеал I_x.

Лемма 2. (а) $x \leq y \iff I_x \subset I_y$

(б) $x = \sup I_x$

Доказательство. (а) Если $x \leq y$, то, очевидно, $I_x \subset I_y$. Если же $x \nleq y$, то по свойству (3) определения f_0-пространства (I.I) существует $x_0 \in X_0$, для которого $x_0 \leq x$, $x_0 \nleq y$. Поэтому $I_x \not\subset I_y$.

(б) Пусть z – верхняя грань I_x. Докажем, что $x \leq z$. Если это не так, то существует $x_0 \leq x$, для которого $x_0 \nleq z$, что противоречит предположению о том, что z –верхняя грань множества I_x. ▨

Назовем f_0-пространство $\langle X, X_0, \leq \rangle$ полным, если всякий идеал в нем равен I_x при некотором $x \in X$. Рассмотренные в I.2 f_0-пространства, как легко проверить, полны.

Частично упорядоченное множество X_0 конечных объектов

конечных объектов f_0 -пространства $\langle X, X_0, \leq \rangle$ обладает, очевидно, следующими свойствами:

(а) В X_0 существует наименьший элемент.

(б) Если x , y , z – элементы X_0 , $x \leq z$, $y \leq z$, то x и y имеют (в X_0) точную верхнюю грань.

Оказывается, что верно и обратное утверждение: всякое частично упорядоченное множество, обладающее свойствами (а) и (б), может быть единственным образом расширено до полного f_0-пространства. Чтобы сформулировать это утверждение точно, нам понадобится следующее определение.

Пусть $\langle X, X_0, \leq \rangle$, $\langle Y, Y_0, \leq \rangle$ – два f_0-пространства. Отображение $f : X \to Y$ назовем изоморфизмом f_0-пространств, если f является взаимно однозначным отображением X на Y , сохраняющим порядок, при котором $f(X_0) = Y_0$.

Предложение I (о пополнении). Пусть $\langle X_0, \leq \rangle$ – частично упорядоченное множество, обладающее свойствами (а) и (б). Тогда:

I. Существует полное пространство $\langle X, X_0, \leq \rangle$, для которого X_0 является множеством конечных объектов, а порядок на X продолжает исходный порядок на X_0 .

2. Такое пространство единственно с точностью до изоморфизма f_0-пространств, тождественного на X_0 .

3. Любое (не обязательно полное) f_0-пространство, множеством конечных объектов которого является X_0, изоморфно части упомянутого полного пространства, причем изоморфизм тождественен на X_0. (Заметим, что если $\langle X, X_0, \leq \rangle$ – f_0-пространство, X' – любое множество, для которого $X_0 \subset X' \subset X$, то $\langle X', X_0, \leq \rangle$ также является f_0-пространством, которое мы называем частью пространства $\langle X, X_0, \leq \rangle$.)

Доказательство. Рассмотрим семейство всех идеалов в час-

тично упорядоченном множестве X_0 , то есть семейство

$$\mathcal{X} = \{ I \subset X_0 \mid (\forall x \in I)(\forall y \leq x)(y \in I) \;\&$$
$$(\forall x, y \in I)(\exists z \in I)(z \text{ - точная верхняя грань } x \text{ и } y \text{ в } X_0) \}$$

Упорядочим множество $\mathcal{X}$ по включению: $I \leq J$, если $I \subset J$.
Вложим X_0 в $\mathcal{X}$, сопоставив каждому $x \in X_0$ множество $I_x = \{ y \mid y \leq x \}$; отображение $x \mapsto I_x$ есть взаимно однозначное отображение X_0 на его образ в $\mathcal{X}$, сохраняющее порядок (ср. лемму 2). Обозначим образ этого вложения через $\mathcal{X}_0$. Покажем, что $\langle \mathcal{X}, \mathcal{X}_0, \leq \rangle$ - f_0-пространство. Наименьшим элементом является $I_\bot = \{ \bot \}$, где $\bot$ - наименьший элемент в X_0 . Если $I_x, I_y \in \mathcal{X}_0, I \in \mathcal{X}$, $I_x \subset I$, $I_y \subset I$, то $x, y \in I$ и, следовательно, в X_0 существует их точная верхняя грань z , причем $z \in I$. Итак, $x \leq z$, $y \leq z$, поэтому $I_x \subset I_z$, $I_y \subset I_z$. Докажем, что I_z - точная верхняя грань I_x и I_y в $\mathcal{X}$. Если $I \in \mathcal{X}$, $I_x \subset I$, $I_y \subset I$, то, как показано, $x, y \in I$ и (так как $I \in \mathcal{X}$) $z \in I$, а значит и $I_z \subset I$. Отождествляя элементы X_0 с их образами в $\mathcal{X}_0$, получаем пространство, множеством конечных объектов которого служит X_0 . Чтобы доказать п.I предложения о пополнении , осталось проверить полноту построенного f_0-пространства. Пусть $\mathcal{J}$ - идеал в $\mathcal{X}$, $\mathcal{J} \subset \mathcal{X}_0$. Соответствующее множество в X_0 является элементом $\mathcal{X}$. Обозначим его J . Докажем, что элемент I множества $\mathcal{X}$ тогда и только тогда входит в $\mathcal{J}$, когда $I \subset J$. В самом деле, $I_{x_0} \in \mathcal{J} \Leftrightarrow x_0 \in J \Leftrightarrow I_{x_0} \subset J$.
Первое утверждение предложения о пополнении доказано.

Пусть теперь $\langle X, X_0, \leq \rangle$ и $\langle X', X_0, \leq \rangle$ - f_0-пространства с одним и тем же множеством конечных объектов и порядком на нем, причем X' полно.[ж)] Докажем, что существует и единствен изоморфизм X на часть X' , тождествен-

ж) Здесь и далее мы пишем кратко "пространство $\mathcal{U}$ " вместо более полной записи "пространство $\langle \mathcal{U}, \mathcal{U}_0, \leq \rangle$ "

ный на X_0. Если $f: X \to X'$ – такой изоморфизм, то идеалы в X_0, задаваемые x и $f(x)$, совпадают. Отсюда вытекает единственность. Докажем существование. Пусть $x \in X$; рассмотрим идеал $I_x \subset X_0$. Он будет идеалом и в пространстве $\langle X', X_0, \leq \rangle$ так как верхние грани двух элементов X_0 в пространствах X и X' совпадают. В силу полноты пространства X' этот идеал порождается некоторым элементом пространства X', который мы и назовем $f(x)$. Монотонность и инъективность f вытекают из леммы 2. Третье утверждение предложения о пополнении доказано.

Чтобы доказать второе утверждение, рассмотрим два полных f_0-пространства $\langle X', X_0, \leq \rangle$ и $\langle X'', X_0, \leq \rangle$ с одним и тем же множеством конечных объектов. По доказанному существуют вложения $f_1 : X' \to X''$ и $f_2 : X'' \to X'$; докажем, что они обратны друг другу. В самом деле, $f_2 \circ f_1$ есть отображение $\langle X', X_0, \leq \rangle$ в себя, сохраняющее порядок и тождественное на X_0, а таким отображением (в силу доказанной единственности) может быть только тождественное.

Предложение о пополнении доказано. ▨

В дальнейшем нам пригодится также следующее свойство полных пространств.

Лемма 3. Пусть V – множество конечных объектов полного f_0-пространства $\langle X, X_0, \leq \rangle$ и любое конечное подмножество множества V имеет точную верхнюю грань в X. Тогда множество V имеет точную верхнюю грань в X.

Доказательство. Каждое конечное подмножество множества V имеет точную верхнюю грань, являющуюся конечным объектом. Рассмотрим множество I тех конечных объектов, которые меньше одной из таких точных верхних граней. Докажем, что это множество – идеал. Если $x \leq \sup(v_1, \ldots, v_n)$, $y \leq \sup(v_1', \ldots, v_m')$,

то и x , и y не превосходят $\sup(v_1,\dots,v_n,v_1',\dots,v_m')$, значит, совместны и $\sup(x,y)\le\sup(v_1,\dots,v_m')$, поэтому $\sup(x,y)\in I$. В силу полноты идеал I равен I_w для некоторого $w\in X$. Очевидно, w - верхняя грань V (так как $V\subset I$); если w'- иная верхняя грань, то $V\subset I_{w'}$ и $I\subset I_{w'}$; значит, $w\le w'$. Лемма 3 доказана. ▨

I.4. Операции над f_0-пространствами.

В этом пункте мы опишем несколько операций, позволяющих получать новые f_0-пространства из уже имеющихся.

I.4.I. Произведение.

Пусть $\langle X, X_0, \leq \rangle$ и $\langle Y, Y_0, \leq \rangle$ – f_0-пространства. Определим новое пространство, объектами которого являются пары $\langle x, y \rangle$ ($x \in X$, $y \in Y$), порядок – покомпонентный, а конечными объектами являются те пары $\langle x, y \rangle$, у которых x и y конечны (в исходных пространствах). Это пространство мы будем называть произведением пространств $\langle X, X_0, \leq \rangle$ и $\langle Y, Y_0, \leq \rangle$ и обозначать $X \times Y$.*)

Лемма I. (а) Произведение f_0-пространств есть f_0-пространство.

(б) Произведение полных f_0-пространств есть полное f_0-пространство.

Доказательство. (а) Если $\perp_X$ – наименьший элемент X, $\perp_Y$ – наименьший элемент Y, то $\langle \perp_X, \perp_Y \rangle$ – наименьший элемент их произведения. Если $\langle x, y \rangle$ и $\langle x', y' \rangle$ – конечные объекты произведения, $\langle z, w \rangle$ – их верхняя грань, то $x, x' \leq z$, $y, y' \leq w$, поэтому существуют и конечны $\sup(x, x')$ и $\sup(y, y')$ и пара $\langle \sup(x, x'), \sup(y, y') \rangle$ будет конечной точной верхней гранью $\langle x, y \rangle$ и $\langle x', y' \rangle$. Если $\langle u, v \rangle \not\leq \langle x, y \rangle$, то $u \not\leq x$ или $v \not\leq y$. Пусть, например, $u \not\leq x$. Тогда существует $u_0 \in X_0$, для которого $u_0 \leq u$, $u_0 \not\leq x$. Тогда $\langle u_0, \perp_Y \rangle \leq \langle u, v \rangle$, $\langle u_0, \perp_Y \rangle \not\leq \langle x, y \rangle$.

(б) Пусть $I \subset X_0 \times Y_0$ – идеал, $J \subset X_0$, $K \subset Y_0$ – его проекции; они являются идеалами в X и Y, как легко

---

*) Мы будем часто употреблять вольность речи, говоря " f_0-пространство X " вместо " f_0-пространство $\langle X, X_0, \leq \rangle$ ", как это делается, например, для топологических пространств.

легко проверить. Докажем, что $I = J \times K$. В самом деле, очевидно, $I \subset J \times K$; если же $j \in J$, $k \in K$, то $\langle j, s \rangle$ и $\langle t, k \rangle$ принадлежат I и $\langle j, k \rangle \leq \sup(\langle j, s \rangle, \langle t, k \rangle) \in I$, поэтому $\langle j, k \rangle \in I$. Пользуясь полнотой X и Y, находим j и k, для которых $J = I_j$, $K = I_k$; тогда $I = J \times K = I_j \times I_k = I_{\langle j, k \rangle}$. Лемма доказана. ▨

I.4.2. Сумма.

Пусть $\langle X, X_0, \leq \rangle$ и $\langle Y, Y_0, \leq \rangle$ – два пространства, причем множества X и Y не пересекаются. Определим новое пространство, объектами которого будут объекты X, объекты Y и дополнительный объект $\perp$, конечными объектами будут $\perp$ и конечные объекты пространств X и Y, отношение $\leq$ определяется так: $\perp$ меньше любого объекта, внутри X и Y порядок сохраняется, и объекты из X не сравнимы с объектами из Y. Построенное пространство мы будем называть суммой пространств X и Y и обозначать $X + Y$. Если X и Y пересекаются, заменим их на непересекающиеся изоморфные пространства X' и Y' и будем считать суммой X и Y пространство $X' + Y'$, описанное выше.

Лемма 2. (а) Сумма f_0-пространств есть f_0-пространство. (б) Сумма полных f_0-пространств есть полное f_0-пространство.

Доказательство. (а) Если a, b – конечные элементы пространства $X + Y$ и они совместны, то или $a = \perp$, или $b = \perp$, или $a, b \in X$, или $a, b \in Y$. Во всех случаях их точная верхняя грань существует и конечна. Если $a \nleq b$ возможны такие случаи: (I) $a \in X, b \in Y$; (2) $a \in Y, b \in X$; (3) $b = \perp$, $a \in X$; (4) $b = \perp$, $a \in Y$; (5) $a, b \in X$; (6) $a, b \in Y$. В первом и третьем случаях, взяв a_0 равным

$\perp_X$ (наименьшему элементу X), получим $a_0 \leq a$, $a_0 \nleq b$; во втором и четвертом случаях возьмем $a_0 = \perp_Y$; в пятом и шестом случаях воспользуемся тем, что X и Y - f_0-пространства.

(б) Пусть I - идеал в построенном пространстве. Он не может одновременно пересекаться с X и Y (так как любой элемент из X несравним с любым элементом из Y), и, следовательно, получается из идеала в X (или в Y) добавлением $\perp$ (или состоит только из $\perp$). Остается воспользоваться полнотой X и Y. ▨

I.4.3. Функциональное пространство.

Пусть X и Y - f_0-пространства; мы построим в этом пункте новое f_0-пространство, элементами которого будут функции из X в Y , но не все, а лишь непрерывные в некоторой естественной топологии.

I.4.3.I. Топология в f_0-пространстве.

Пусть $\langle X, X_0, \leq \rangle$ - f_0-пространство. С каждым конечным элементом $x_0 \in X_0$ свяжем множество $\Gamma x_0 = \{x \in X \mid x_0 \leq x\}$ всех его продолжений. Если x_0 и x_0' - два конечных элемента, то либо Γx_0 и $\Gamma x_0'$ не пересекаются, либо $\Gamma x_0 \cap \Gamma x_0' = \Gamma_{\sup(x_0, x_0')}$. Поэтому семейство множеств Γx_0 (для всех $x_0 \in X_0$) можно объявить базой топологии. Этой топологией мы и будем всегда снабжать f_0-пространства. Открытые множества этой топологии имеют следующее простое описание.

Лемма 3. Множество $A \subset X$ открыто тогда и только тогда, когда одновременно выполнены два следующих условия:

(I) $x \in A,\ x \leq y \Rightarrow y \in A$;

(2) $x \in A \Rightarrow (\exists x_0 \in X_0)(x_0 \leq x \ \&\ x_0 \in A)$

Доказательство. Для базовых множеств условия (I) и (2) выполнены, следовательно, они выполнены и для любого открытого множества. Обратно, пусть A - множество, удовлетворяющее ус-

ловиям (I) и (2). Рассмотрим объединение A' множеств Γ_{x_0} при всех $x_0 \in A$. Условие (I) гарантирует, что $A' \subset A$. Условие (2) гарантирует, что $A \subset A'$. ▨

I.4.3.2. Непрерывные отображения.

Пусть $\langle X, X_0, \leq \rangle$, $\langle Y, Y_0, \leq \rangle$ - два f_0-пространства, снабженных указанными топологиями, $f: X \to Y$ - всюду определенная функция из X в Y. Следующая лемма дает простой критерий непрерывности функции f.

Лемма 4. Функция f непрерывна тогда и только тогда, когда одновременно выполнены два следующих условия:

(I) $x \leq x' \Rightarrow f(x) \leq f(x')$;

(2) $y_0 \in Y_0,\ y_0 \leq f(x) \Rightarrow (\exists x_0 \in X_0)(x_0 \leq x \,\&\, y_0 \leq f(x_0))$.

Доказательство. Пусть f непрерывна, $x \leq x'$, $f(x) \not\leq f(x')$. Тогда существует $y_0 \in Y_0$, для которого $y_0 \leq f(x)$, $y_0 \not\leq f(x')$. Тогда x содержится в $f^{-1}(\Gamma_{y_0})$, а x' не содержится, что, согласно лемме 3, противоречит его открытости. Если же f непрерывна, $y_0 \in Y_0$, $y_0 \leq f(x)$, то $x \in f^{-1}(\Gamma_{y_0})$ и по лемме 3 существует $x_0 \in X_0$, для которого $x_0 \leq x$ и $x_0 \in f^{-1}(\Gamma_{y_0})$, то есть $y_0 \leq f(x_0)$.

Пусть теперь условия (I) и (2) выполнены; докажем непрерывность f. Достаточно проверить открытость прообраза одного базового множества Γ_{y_0} с помощью леммы 3. В самом деле, если $x \leq x'$, $x \in f^{-1}(\Gamma_{y_0})$, то $y_0 \leq f(x) \leq f(x')$ и $x' \in f^{-1}(\Gamma_{y_0})$. Кроме того, если $x \in f^{-1}(\Gamma_{y_0})$, то $y_0 \leq f(x)$ и по свойству (2) функции f существует $x_0 \in X_0$, для которого $x_0 \leq x$ и $y_0 \leq f(x_0)$, то есть $x_0 \in f^{-1}(\Gamma_{y_0})$. ▨

I.4.3.3. Свойства непрерывных функций.

Непрерывная функция однозначно задается своими значениями на конечных объектах, как показывает следующая

Лемма 5. (а) Пусть f – непрерывная функция из f_0-пространства $\langle X, X_0, \leq\rangle$ в f_0-пространство $\langle Y, Y_0, \leq\rangle$. Тогда для всех $x \in X$ выполнено равенство

$$f(x) = \sup \{ f(x_0) \mid x_0 \leq x \};$$

в частности, $\sup$ существует.

(б) Если g – функция из X_0 в Y, являющаяся монотонной ($x_0 \leq x_0' \Rightarrow g(x_0) \leq g(x_0')$), а Y полно, то g может быть продолжена до непрерывной функции из X в Y.

Доказательство. (а) Очевидно, $f(x)$ – верхняя грань множества $\{ f(x_0) \mid x_0 \leq x\}$. Пусть y – любая другая верхняя грань и $f(x) \not\leq y$. Тогда существует $y_0 \in Y_0$, для которого $y_0 \leq f(x)$, $y_0 \leq y$. В силу непрерывности f существует $x_0 \in X_0$, для которого $x_0 \leq x$, $y_0 \leq f(x_0)$. Теперь получаем $y_0 \leq f(x_0) \leq y$ (y – верхняя грань), что противоречит $y_0 \not\leq y$.

(б) Пусть g – монотонная функция из X_0 в Y. Сопоставим каждому $x \in X$ множество

$$B_x = \{ y_0 \in Y_0 \mid (\exists x_0 \in X_0)[x_0 \leq x \ \& \ y_0 \leq g(x_0)]\}$$

Докажем, что это идеал в Y. В самом деле, вместе с каждым элементом он содержит все меньшие; если y_0, $y_0' \in B_x$, то существуют $x_0, x_0' \leq x$, для которых $y_0 \leq g(x_0)$, $y_0' \leq g(x_0')$. Так как x_0, x_0' совместны, можно рассмотреть $z = \sup(x_0, x_0')$; имеем $y_0 \leq g(x_0) \leq g(z)$, $y_0' \leq g(x_0') \leq g(z)$ (g монотонна), значит, y_0 и y_0' совместны, $\sup(y_0, y_0') \leq g(z)$ и поэтому $\sup(y_0, y_0') \in I$.

В силу полноты Y идеал B_x состоит из всех объектов, меньших некоторого; этот последний мы и возьмем в качестве $f(x)$. Функция f продолжает g: если $x \in X_0$, то $B_x = \{ y_0 \in Y_0 \mid y_0 \leq g(x_0)\}$ Проверим непрерывность f, пользуясь леммой 4. Если $x \leq x'$, то $B_x \subset B_{x'}$, поэто-

му $f(x) \le f(x')$. Если $y_0 \in Y$, $y_0 \le f(x)$, то $y_0 \in B_x$ и поэтому $\exists x_0 \in X [(x_0 \le x) \,\&\, y_0 \le g(x_0)]$. Осталось воспользоваться тем, что g продолжает f. Лемма 5 доказана. ▨

I.4.3.4. Функциональное пространство. Конечные элементы.

Пусть $\langle X, X_0, \le \rangle$, $\langle Y, Y_0, \le \rangle$ – f_0-пространства. Определим пространство $C(X,Y)$. Его объектами будут непрерывные всюду определенные функции из X в Y. Порядок поточечный: $f \le g$, если для всех $x \in X$ выполнено $f(x) \le g(x)$ (в смысле порядка на Y). Более сложно описать, какие объекты будут конечными. Пусть $x_0 \in X_0$, $y_0 \in Y_0$. Определим функцию $(x_0 \mapsto y_0) : X \to Y$ следующей формулой:

$$(x_0 \mapsto y_0)(x) = \begin{cases} y_0, & \text{если } x_0 \le x \\ \bot_Y, & \text{если } x_0 \not\le x. \end{cases}$$

Эта функция удовлетворяет условиям (I) и (2) леммы 4, и, следовательно, непрерывна. Точные верхние грани конечных семейств функций вида $(x_0 \mapsto y_0)$ (для тех семейств, для которых они существуют) мы будем считать конечными объектами пространства $C(X,Y)$. Определение пространства $C(X,Y)$ завершено.

Лемма 6. (а) Пространство $C(X,Y)$ является f_0-пространством.

(б) Если пространство Y полно, то для всякого пространства X пространство $C(X,Y)$ полно.

Прежде чем доказывать эту лемму, дадим более явное описание конечных элементов пространства $C(X,Y)$.

Лемма 7. Множество $\{(x_1 \mapsto y_1), \ldots, (x_n \mapsto y_n)\}$ тогда и только тогда совместно (имеет верхнюю грань) в $C(X,Y)$, когда для всякого $I \subset \{1,\ldots,n\}$, для которого $\{x_i \mid i \in I\}$

совместно в X, множество $\{y_i \mid i \in I\}$ совместно в Y. Всякое совместное множество указанного вида имеет точную верхнюю грань.

Доказательство. Пусть f – верхняя грань множества $\{(x_1 \mapsto y_1), \ldots, (x_n \mapsto y_n)\}$, $I \subset \{1, \ldots, n\}$, $\{x_i \mid i \in I\}$ совместно и $x \geq x_i$ для всех $i \in I$. Тогда $f(x) \geq (x_i \mapsto y_i)(x) = y_i$ и, следовательно, $\{y_i \mid i \in I\}$ совместно. Обратно, пусть условие выполнено. Рассмотрим функцию $(x_1 \mapsto y_1, \ldots, x_n \mapsto y_n)$ определенную формулой

$$(x_1 \mapsto y_1, \ldots, x_n \mapsto y_n)(x) = \sup \{y_i \mid x_i \leq x\}$$

(точная верхняя грань в правой части по предположению существует). С помощью леммы 4 легко проверить ее непрерывность. Очевидно, $(x_i \mapsto y_i)(x) \leq (x_1 \mapsto y_1, \ldots, x_n \mapsto y_n)(x)$ поэтому построенная функция является верхней гранью множества $\{(x_1 \mapsto y_1), \ldots, (x_n \mapsto y_n)\}$. Проверим, что эта верхняя грань – точная. В самом деле, если f – верхняя грань множества $\{(x_1 \mapsto y_1), \ldots, (x_n \mapsto y_n)\}$, то $f(x_i) \geq y_i$ и $f(x) \geq y_i$ для всех тех i, для которых $x_i \leq x$. ▨

Учитывая лемму 7, можно сказать, что конечными объектами пространства $C(X, Y)$ являются функции вида $(x_1 \mapsto y_1, \ldots, x_n \mapsto y_n)$, где x_i и y_i – наборы конечных объектов пространств X и Y, для которых выполнено указанное в лемме 7 условие. Теперь мы можем дать

Доказательство леммы 6. (а) Проверим, что условия, указанные в определении f_c-пространства, выполнены. Наименьшим объектом является объект $(\bot_X \to \bot_Y)$. Если $(x_1 \mapsto y_1, \ldots) \leq f$ и $(u_1 \mapsto v_1, \ldots) \leq f$, то все $(x_i \mapsto y_i) \leq f$ и все $(u_i \mapsto v_i) \leq f$, значит, существует $\sup (x_1 \mapsto y_1, \ldots, u_1 \mapsto v_1, \ldots)$, который и будет конечной точной верхней гранью рассмотренных объектов.

Пусть теперь $f \nleq g$, то есть $f(x) \nleq g(x)$ для некоторого x. Этот x можно считать конечным, сославшись на пункт (а) леммы 5. Теперь возьмем конечное u, для которого $u \leq f(x)$, но $u \nleq g(x)$. Имеем $(x \mapsto u) \leq f$, $(x \mapsto u) \nleq g$. Итак, мы проверили, что $C(X,Y)$ действительно является f_0-пространством.

(б) Докажем теперь полноту пространства $C(X,Y)$. Пусть K - идеал в $C(X,Y)$. Для каждой точки $x \in X$ рассмотрим множество K_x всех значений функций из K на x. Так как элементами K являются конечные объекты $C(X,Y)$, то элементами K_x будут конечные объекты Y. Докажем, что K_x - идеал в Y. Пусть $y \in K_x$, $z \leq y$, $z \in Y_0$. Докажем, что $z \in K_x$. Так как $y \in K_x$, то $y = f(x)$ и $z \leq f(x)$ для некоторой функции f из K. В силу непрерывности f имеем $z \leq f(x_0)$ для некоторого $x_0 \in X_0$, $x_0 \leq x$. Функция $g = (x_0 \mapsto z)$ меньше f в смысле порядка на $C(X,Y)$ поэтому $g \in K$, а $z = g(x) \in K_x$. Пусть теперь y, $z \in K_x$, $y = f(x)$, $z = g(x)$, f, $g \in K$. Раз f, $g \in K$, то существует $h \in K$, для которого $f \leq h$, $g \leq h$. Тогда $f(x) \leq h(x)$, $g(x) \leq h(x)$ и $h(x) \in K_x$, значит, y и z имеют мажоранту в K_x, поэтому они совместны и их точная верхняя грань лежит в K_x. Итак, K_x - идеал; так как Y полно, то $K_x = I_{t(x)}$, где t - некоторая функция из X в Y. Докажем, что t непрерывна. Если $x \leq x'$, то $f(x) \leq f(x')$ для любой функции $f \in K$, поэтому $K_x \subset K_{x'}$ и $t(x) \leq t(x')$. Если $y_0 \leq t(x)$, $y_0 \in Y_0$ то $y_0 \in K_x$ и $y_0 = f(x)$ для некоторой $f \in K$; так как f непрерывна, а y_0 конечен, то существует $x_0 \in X_0$, для которого $y_0 \leq f(x_0) \leq f(x) = y_0$ и $y_0 \in K_{x_0}$, то есть $y_0 \leq t(x_0)$. Осталось доказать, что функция

$s=(x_1\mapsto y_1,\dots,x_n\mapsto y_n)$ тогда и только тогда принадлежит K, когда $s(x)\le t(x)$ для всех x. Если $s\in K$, то $s(x)\in K_x$ и $s(x)\le t(x)$. Напротив, если $s(x)\le t(x)$ при всех x, то $(x_1\mapsto y_1)(x)\le t(x)$, $y_1\le t(x_1)$, $y_1\in K_{x_1}$, $y_1=f(x_1)$ для некоторой $f\in K$, $(x_1\mapsto y_1)\le f\in K$ и поэтому $(x_1\mapsto y_1)\in K$. Аналогично $(x_i\mapsto y_i)\in K$ при всех i, поэтому их точная верхняя грань – функция s – также принадлежит K. Лемма 6 доказана. ▨

I.4.4. Стандартные изоморфизмы.

Лемма 8. Имеют место естественные изоморфизмы f_0-пространств

(а) $C(X,C(Y,Z))\simeq C(X\times Y,Z)$;

(б) $C(X,Y\times Z)\simeq C(X,Y)\times C(X,Z)$,

задаваемые формулами $f\longmapsto \tilde f$, $\tilde f:\langle x,y\rangle\longmapsto[f(x)](y)$

и $f\mapsto\langle f_Y,f_Z\rangle$ где $f(x)=\langle f_Y(x),f_Z(x)\rangle$.

Напомним, что изоморфизмом f_0-пространств называется взаимно однозначное отображение множеств объектов, сохраняющее порядок и конечность (I.3).

Доказательство. (а) Покажем, что описанная формула задает элемент $\tilde f$ из $C(X\times Y,Z)$. Монотонность (условие I из леммы 4) очевидна. Проверим условие 2 этой леммы. Пусть $z\in Z_0$ (множеству конечных объектов пространства Z), $z_0\le[f(x)](y)$. Тогда (ибо $f(x)\in C(Y,Z)$) существует $y_0\le y$, $y_0\in Y_0$, для которого $z_0\le[f(x)](y_0)$ Теперь ясно, что $(y_0\mapsto z_0)\le f(x)$ и в силу непрерывности f существует $x_0\in X_0$, $x_0\le x$, для которого $(y_0\mapsto z_0)\le f(x_0)$, $z_0\le[f(x_0)](y_0)=\tilde f(x_0,y_0)$. Непрерывность $\tilde f$ доказана.

Обратное отображение ставит в соответствие функции $g\in C(X\times Y,Z)$ функцию $\check g: x\longmapsto g_x$

где $g_x : y \mapsto g(x,y)$. Функция g_x принадлежит $C(Y, Z)$ так как если $z_0 \in Z_0$, $z_0 \le g_x(y) = g(x,y)$, то существуют $x_0 \le x$, $y_0 \le y$, $x_0 \in X_0$, $y_0 \in Y_0$, для которых $z_0 \le g(x_0, y_0) \le g(x, y_0) = g_x(y_0)$. Функция $x \mapsto g_x$ принадлежит $C(X, C(Y, Z))$, так как если $(y_1 \mapsto z_1, \ldots) \le g_x$, $y_i \in Y_0$, $z_i \in Z_0$, то $z_1 \le g(x, y_1), \ldots$ и существуют $x_i \in X_0$, $x_i \le x$, для которых $z_i \le g(x_i, y_i)$, и взяв $x_0 = \sup x_i$, имеем $z_i \le g(x_0, y_i)$ для всех i, то есть $(y_i \mapsto z_i) \le g_{x_0}$ для всех i и $(y_1 \mapsto z_1, \ldots) \le g_{x_0}$

Итак, обратное отображение определено корректно. Сохранение порядка очевидно; проверим, что конечные объекты переходят в конечные. В $C(X, C(Y, Z))$ конечными объектами являются точные верхние грани совместных конечных множеств объектов вида $(x_1 \mapsto (y_1 \mapsto z_1, \ldots, y_n \mapsto z_n))$ (x_1, y_i, z_i - конечные объекты X, Y, Z). Так как указанный объект равен $\sup((x_1 \mapsto (y_1 \mapsto z_1)), \ldots, (x_1 \mapsto (y_n \mapsto z_n)))$, то можно ограничиться случаем $n = 1$. Эти объекты переходят при описанном соответствии в объекты вида $\langle x_1, y_1 \rangle \mapsto z_1$, точные верхние грани которых и образуют конечные объекты в $C(X \times Y, Z)$.

(б) Функции f_Y и f_Z непрерывны, так как являются композициями функции f и (непрерывных) проекций $Y \times Z \to Y$ и $Y \times Z \to Z$. Обратно, если f_Y и f_Z непрерывны, то и f непрерывна - как легко проверить, топология в $Y \times Z$ является произведением топологий в Y и Z. Конечные объекты в $C(X, Y \times Z)$ являются точными верхними гранями объектов вида $(x_0 \mapsto \langle y_0, z_0 \rangle)$, которым соответствуют в $C(X, Y) \times C(X, Z)$ объекты вида $\langle (x_0 \mapsto y_0), (x_0 \mapsto z_0) \rangle$, которые конечны. Напротив, объекту $\langle (x_1 \mapsto y_0), (x_2 \mapsto z_0) \rangle$ соответствует объект $(x_1 \mapsto \langle y_0, \bot_Z \rangle, x_2 \mapsto \langle \bot_Y, z_0 \rangle)$, который также конечен. ▨

I.5. Эффективные f_0 -пространства.

В этом пункте мы опишем, каким образом f_0 -пространство можно снабдить дополнительной структурой, позволяющей говорить о вычислимости его объектов.

I.5.I. Определение эффективного f_0 -пространства. Примеры.

Пусть $\langle X, X_c, \leq \rangle$ - f_0-пространство, ν - натуральная нумерация множества X_c (всюду определенное отображение $\mathbb{N}$ на X_0 ; если $\nu(n)=x$, то n называется номером x).
Пусть множества $\{\langle m,n\rangle \mid \nu(m) \leq \nu(n)\}$ и $\{\langle m,n\rangle \mid \nu(m)$ и $\nu(n)$ совместны$\}$ разрешимы и существует вычислимая функция f из $\mathbb{N}^2$ в $\mathbb{N}$, для которой $\nu(f(m,n)) = \sup(\nu(m), \nu(n))$ для тех m и n, для которых $\nu(m)$ и $\nu(n)$ совместны.

В этом случае четверку $\langle X, X_0, \leq, \nu \rangle$ мы будем называть эффективным f_0 -пространством.

Очевидно, в эффективном пространстве множество конечных объектов не более чем счетно, а множество всех объектов не более чем континуально. Мы не будем различать эффективных f_0 -пространств, получающихся заменой нумерации на вычислимо эквивалентную (определение см., например, в).

В f_0-пространствах из I.2 нетрудно ввести естественным образом структуры эффективных пространств. Приведем для полноты описания соответствующих нумераций.

В I.2.I $\nu(n) = \perp$ для любого n.

В I.2.2 $\nu(n) = \perp$ при $n \neq 0$, $\nu(0) = *$.

В I.2.3 $\nu(0) = \perp$, $\nu(n) = n-1$ при $n > 0$.

В I.2.4 выберем и зафиксируем какую-нибудь вычислимую нумерацию двоичных слов в качестве ν.

В I.2.5 выберем в качестве ν одну из стандартных нумераций конечных множеств (например, описанную в [11], с.97).

В I.2.6. отождествим частичные функции со значениями 0 и I со словами из символов 0, I, $*$, последний символ в которых отличен от $*$, и рассмотрим произвольную вычислимую нумерацию таких слов.

В I.2.7. поступаем по аналогии с пространствами Ω и Ξ .

I.5.2. Структуры эффективных пространств на произведении, сумме и функциональном пространстве.

Пусть заданы эффективные f_0-пространства $\langle X, X_0, \leq, \nu \rangle$ и $\langle Y, Y_0, \leq, \mu \rangle$. Тогда на их произведении, сумме, а также на пространстве $C(X, Y)$ возникают структуры эффективных f_0-пространств.

Произведение. В $X \times Y$ конечными объектами являются элементы $X_0 \times Y_0$. Пусть $\langle \xi, \eta \rangle : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ - взаимно однозначное вычислимое соответствие между $\mathbb{N}$ и $\mathbb{N} \times \mathbb{N}$. В качестве нумерации $X_0 \times Y_0$ возьмем функцию τ :

$$\tau(n) = \langle \nu(\xi(n)), \mu(\eta(n)) \rangle$$

Сумма. В $X+Y$ конечными объектами являются $\perp$ и конечные объекты X и Y . В качестве нумерации возьмем функцию τ :

$$\tau(0) = \perp, \ \tau(2n+1) = \nu(n), \ \tau(2n+2) = \mu(n).$$

Пространство $C(X,Y)$. В $C(X,Y)$ конечными объектами являются точные верхние грани семейств объектов вида $(x_i \mapsto y_i)$, $x_i \in X_0, y_i \in Y_0$. Все такие семейства можно занумеровать, например, так: если $\nu(n_i) = x_i$, $\nu(m_i) = y_i$, k - номер кортежа $\langle n_1, m_1, \ldots, n_s, m_s \rangle$ в стандартной нумерации кортежей натуральных чисел, то мы будем считать k номером семейства

$$\{(x_1 \mapsto y_1), \ldots, (x_s \mapsto y_s)\}.$$

Лемма I. Множество тех k , которые являются номерами совместных семейств, разрешимо.

Доказательство. В самом деле, лемма 7 из I.4 позволяет вы-

яснить совместность семейства за конечное число проверок (равное числу подмножеств $I \subset \{1,2,\ldots,s\}$). Эффективность каждой проверки обеспечивается тем, что X и Y – эффективные f_0 -пространства.

Теперь мы можем ввести нумерацию конечных объектов пространства $C(X,Y)$, положив, что тем k , которые являются номерами (в описанном смысле) совместных семейств, соответствуют точные верхние грани этих семейств, а остальным k соответствует наименьший элемент пространства $C(X,Y)$.

Лемма 2. Описанная нумерация удовлетворяет требованиям, перечисленным в определении эффективного f_0-пространства.

Доказательство. Пусть мы хотим выяснить, верно ли, что

$$(x_1 \mapsto y_1, \ldots, x_n \mapsto y_n) \leq (u_1 \mapsto v_1, \ldots, u_m \mapsto v_m)$$

где x_i , y_i , u_i , v_i заданы своими номерами. Достаточно ограничиться случаем $n=1$, так как $\sup(a,b) \leq c \Leftrightarrow (a \leq c \,\&\, b \leq c)$. Чтобы узнать, верно ли, что $(x_1 \mapsto y_1) \leq (u_1 \mapsto v_1, \ldots, u_m \mapsto v_m)$ надо вычислить значение правой части на x_1 , для чего найти те i , для которых $u_i \leq x_1$, и взять точную верхнюю грань соответствующих y_i . (Возможность эффективного выполнения этих действий, т.е. нахождения соответствующих номеров, обеспечивается эффективностью пространств X и Y .) Затем эту грань надо сравнить с y_1 .

Для определения совместности двух конечных объектов пространства $C(X,Y)$, заданных их номерами, нужно воспользоваться леммой I. Наконец, точную верхнюю грань двух совместных конечных объектов можно найти, приписав друг к другу кортежи, соответствующие этим объектам. Лемма 2 доказана.

Нетрудно проверить, что при описанных выше стандартных изоморфизмах $C(X, C(Y,Z)) \simeq C(X \times Y, Z)$

и $C(X, Y\times Z) \simeq C(X,Y)\times C(X,Z)$ нумерации в левой и правой части, построенные описанным способом, переходят друг в друга (с точностью до вычислимой эквивалентности нумераций).

I.5.3. Вычислимые объекты. Относительная вычислимость.

Пусть $\langle X, X_0, \le, \nu\rangle$ - эффективное f_0-пространство. Объект $x\in X$ назовем вычислимым, если множество $\{n \mid \nu(n)\le x\}$ номеров всех меньших его конечных объектов перечислимо.

Согласно определению эффективного f_0-пространства всякий конечный объект вычислим. Ясно также, что множество вычислимых объектов в f_0-пространстве не более чем счетно.

Лемма 3. Пусть X, Y - эффективные пространства, $f\in C(X,Y)$ и $x\in X$ - вычислимые объекты. Тогда $f(x)$ - вычислимый объект в Y. (Говоря о вычислимости f, мы имеем в виду описанную в I.5.2 структуру эффективного f_0-пространства в $C(X,Y)$.)

Доказательство. Так как f непрерывно, то для всех $y_0\in Y$ имеем

$$y_0\le f(x) \iff (\exists x_0\in X_0)((x_0\le x)\,\&\,(y_0\le f(x_0))) \iff$$
$$(\exists x_0\in X_0)(((x_0\mapsto y_0)\le f)\,\&\,(x_0\le x))$$

и осталось сослаться на вычислимость f и x. ▨

Пусть $\langle X, X_0, \le, \nu\rangle$ и $\langle Y, Y_0, \le, \mu\rangle$ - два эффективных f_0-пространства. Будем говорить, что $x\in X$ вычислим относительно $y\in Y$, если существует вычислимый объект $f\in C(Y,X)$, для которого $f(y)=x$.

Лемма 4. Объект $x\in X$ вычислим тогда и только тогда, когда он вычислим относительно любого объекта y в любом эффективном пространстве Y.

Доказательство. Если $x \in X$ вычислим, Y - любое эффективное пространство, то функция f из $C(Y,X)$ тождественно равная x, вычислима, так как $(u \mapsto v) \le f \Leftrightarrow v \le x$. Чтобы доказать обратную импликацию, достаточно взять в качестве y вычислимый объект и применить лемму 3. ▨

В дальнейшем нам потребуется также следующая

Лемма 5. Пусть X, Y, Z - эффективные f_0-пространства, $g \in C(X,Y)$ и $h \in C(Y,Z)$ - вычислимые объекты. Тогда объект $h \circ g \in C(X,Z)$ вычислим.

Доказательство. В самом деле, если $x \in X_0$, $z \in Z_0$ - конечные объекты пространств X и Z, то

$$(x_0 \mapsto z_0) \le h \circ g \Leftrightarrow (\exists y_0 \in Y_0)((x_0 \mapsto y_0) \le g \ \& \ (y_0 \mapsto z_0) \le h). ▨$$

I.5.4. Примеры вычислимых объектов.

Рассмотрим, какие объекты вычислимы в указанных в п. I.2 f_0-пространствах и в пространствах, из них получающихся. В пространстве $\mathbb{N}_\perp$ вычислимы все объекты, так как все они конечны. В пространстве Ω вычислимы все конечные последовательности, а также вычислимые (в обычном смысле) бесконечные последовательности. В пространстве Ξ частичных функций со значениями 0 и I и в пространстве $\mathbb{F}$ частичных функций из $\mathbb{N}$ в $\mathbb{N}$ вычислимы частично рекурсивные функции. В пространстве $2^{\mathbb{N}}$ подмножеств $\mathbb{N}$ вычислимы перечислимые множества.

Вычислимые объекты в $C(2^{\mathbb{N}}, 2^{\mathbb{N}})$ суть вычислимые операции (операторы перечисления в смысле [11], с. 192), вычислимые объекты из $C(\mathbb{F},\mathbb{F})$ - вычислимые операторы (рекурсивные операторы в смысле [11], с. 194); вычислимые объекты из $C(\mathbb{F},\mathbb{N}_\perp)$ - рекурсивные функционалы (в смысле [11], с. 459). Вычислимые объекты из $C(\Omega,\Omega)$ - алгоритмические операторы (в смысле [2], с. 33). Вычислимые объекты из $C(\mathbb{N}_\perp,\mathbb{N}_\perp)$- либо тождественно равные одному и тому же числу функции, либо функции, равные

$\perp$ на $\perp$, совпадающие с некоторой частично рекурсивной функцией f из $\mathbb{N}$ в $\mathbb{N}$ на тех n, на которых f определена, и равные $\perp$ на тех n, на которых f не определена.

Более подробно мы рассмотрим вычислимые объекты некоторых пространств в дальнейшем, в связи с определением энтропии.

I.5.5. Перечисление множества вычислимых объектов.

В дальнейшем нам понадобится следующее

Предложение I. Для всякого полного эффективного f_0-пространства X существует вычислимое отображение из $C(\mathbb{N}_\perp, X)$, образом которого является множество всех вычислимых объектов пространства X.

Доказательство. Пусть ν – нумерация всех конечных объектов эффективного пространства X. Для каждого i рассмотрим i-ое перечислимое множество W_i (в стандартной нумерации перечислимых множеств натуральных чисел). Множество $\nu(W_i)$ может быть несовместным; мы преобразуем его в множество K_i, которое всегда будет совместным и будет совпадать с $\nu(W_i)$ если последнее совместно. (Совместным мы называем множество, любое конечное подмножество которого имеет точную верхнюю грань. Множества K_i определяются так. Перечисляя $W_i = \{a_0, a_1, \ldots\}$ мы каждый следующий элемент $\nu(a_n)$ проверяем на совместность с $\nu(a_0), \ldots, \nu(a_{n-1})$ (это возможно по определению f_0-пространства); если $\{\nu(a_0), \ldots, \nu(a_{n-1}), \nu(a_n)\}$ совместно, то включаем $\nu(a_n)$ в K_i; как только обнаружится несовместность, больше никаких элементов в K_i мы не включаем.

Искомую функцию из $C(\mathbb{N}_\perp, X)$ определим теперь так:

$$f(\perp) = \perp; \quad f(i) = \sup K_i$$

(В силу леммы 3 из I.3 $\sup K_i$ существует.)

В силу леммы 4 из I.4 эта функция непрерывна; всякий вы-

числимый объект попадает в ее образ, так как представляет собой точную верхнюю грань множества меньших его конечных объектов (лемма 2 из I.3), а множество их номеров перечислимо и встречается среди W_i. Осталось проверить вычислимость функции f. Объект $(\perp \mapsto a)$ меньше f, если и только если $a = \perp$; объект $(n \mapsto x)$ меньше f тогда и только тогда, когда $x \leq \sup K_n$, то есть (см. доказательство леммы 3 из I.3) когда существуют такие $b_1, \ldots, b_m \in K_n$ что $x \leq \sup(b_1, \ldots, b_m)$. А последнее свойство перечислимо в силу построения K_n и эффективности пространства X. ▨

<u>Следствие предложения I</u>. Пусть X, Y – эффективные f_0-пространства, Y полно. Тогда существует вычислимый объект f из $C(\mathbb{N}_\perp \times X, Y)$, сечения $f_n : x \mapsto f(n, x)$ которого исчерпывают множество вычислимых объектов пространства $C(X, Y)$.

<u>Доказательство</u>. По доказанному предложению имеется вычислимое отображение $F \in C(\mathbb{N}_\perp, C(X, Y))$, образ которого состоит из всех вычислимых объектов пространства $C(X, Y)$ Остается воспользоваться изоморфизмом $C(\mathbb{N}_\perp, C(X, Y)) \simeq C(\mathbb{N}_\perp \times X, Y)$, описанным в I.4.4 (лемма 8). ▨

I.6. Объем на f_0 -пространствах.

Пусть X – эффективное f_0-пространство, X_c – множество конечных объектов этого пространства, ℓ – функция на X_c с натуральными значениями, обладающая следующими свойствами:

(I) $x_1 \le x_2 \Rightarrow \ell(x_1) \le \ell(x_2)$

(2) $\ell(x)$ можно эффективно найти по номеру объекта x.

Функцию с такими свойствами мы будем называть объемом на пространстве X.

Основные примеры объемов.

I. $X = \mathbb{N}_\perp$, $\ell(\perp) = 0$, $\ell(n) = [\log_2(1+n)]$

($[p]$ обозначает целую часть p).

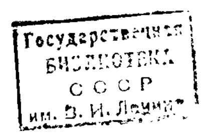
2. $X = \Omega$, $\ell(x)$ = длина последовательности x.

3. $X = \Xi$, $\ell(x)$ = число элементов в области определения функции x.

Таким образом, мы ввели необходимое нам для дальнейшего понятие полного эффективного f_0-пространства и понятие объема на нем. В дальнейшем мы будем под пространством понимать полное эффективное f_0-пространство, если нет специальных оговорок; кроме того, мы будем продолжать сокращенно писать "пространство X" вместо более полного "пространство $\langle X, X_c, \le, \nu \rangle$".

Глава 2. Задачи и их энтропия.

В этой главе на основе понятия f_0-пространства мы определим понятие задачи и понятие энтропии задачи - уточнение интуитивного представления о сложности отыскания решения задачи.



2.1. Определение задачи. Монотонные и разрешимые задачи.

Задачей назовем пару $\alpha = \langle X, A \rangle$, где X - пространство, а A - некоторое подмножество X.

Говоря неформально, задача состоит в отыскании объекта пространства X, входящего в A.

Пространство X мы будем называть пространством задачи α, а объекты, входящие в A - решениями задачи α.

Задачу $\alpha = \langle X, A \rangle$ назовем монотонной, если из $x \leq y$, $x \in A$ следует $y \in A$, то есть если любой объект, продолжающий некоторое решение, сам есть решение. Большая часть задач, которые мы рассматриваем, монотонны.

Задачу $\alpha = \langle X, A \rangle$ назовем разрешимой, если существует вычислимый объект пространства X, являющийся ее решением.

В дальнейшем мы расклассифицируем разрешимые задачи по "сложности их решения", определив понятие энтропии задачи.

2.2. Способы описания. Сложность задачи при данном способе описания.

Пусть X , Y - пространства, ℓ - объем на пространстве X .

Способом описания объектов Y с помощью объектов X назовем любой вычислимый объект пространства $C(X,Y)$.

Пусть даны способ описания $f \in C(X,Y)$ и задача $\alpha = \langle Y, A \rangle$ в пространстве Y . Рассмотрим число $K_f(\langle Y, A \rangle) = \inf \{\ell(x_0) | x_0$ - конечный объект пр-ва X , $f(x_0) \in A\}$ (как обычно, полагаем $\inf \emptyset = \infty$), называемое сложностью задачи α при способе описания f .

Имеет место следующая простая

Лемма I. (а) Если $K_f(\alpha) < \infty$, то задача α разрешима.
(б) Если задача α разрешима, то существует способ описания f , при котором $K_f(\alpha) < \infty$.
(напомним, что пространства X , Y и объем на X фиксированы)

Доказательство. (а) Если $K(\alpha) < \infty$, то существует конечный объект $x_0 \in X$, для которого $f(x_0) \in A$. Тогда $f(x_0)$ будет вычислимым решением задачи α .

(б) Если задача α разрешима, y - ее вычислимое решение, то функция $f \in C(X,Y)$, тождественно равная y , будет искомым способом кодирования. ▨

2.3. Необходимые и достаточные условия для существования оптимального способа описания.

Различные способы описания приводят, естественно, к различным сложностям одной и той же задачи. Нас интересует вопрос о том, когда среди всех способов описания существует оптимальный - дающий в каком-то смысле наименьшую сложность. В этом пункте мы уточним этот вопрос и дадим ответ на него.

Пусть X, Y - пространства, ℓ - объем на X, f и g - два способа описания объектов из Y с помощью объектов из X. Будем говорить, что способ f эффективнее способа g, если существует такая константа C, что для любой задачи $\alpha = \langle Y, A\rangle$ в пространстве Y имеет место неравенство $K_f(\alpha) \leq K_g(\alpha) + C$. Способ f назовем оптимальным способом описания объектов Y с помощью объектов X, если он эффективнее любого другого способа описания $g \in C(X,Y)$. (Заметим, что в соответствии с нашим определением каждый способ описания эффективнее самого себя.) Пространство X с объемом ℓ назовем регулярным, если для всякого пространства Y существует оптимальный способ описания объектов Y с помощью объектов X. Следующее предложение дает легко проверяемый критерий регулярности пространства.

Предложение I. Пространство X с объемом ℓ регулярно тогда и только тогда, когда существует такой способ описания f объектов пространства $X \times \mathbb{N}_\perp$ с помощью объектов X, что выполнено свойство

$$(\forall n \in \mathbb{N})(\exists C)(\forall x \in X_0)(K_f(\langle X \times \mathbb{N}_\perp, \{\langle x_0, n\rangle\}\rangle) \leq \ell(x_0) + C) \quad (*)$$

Доказательство. Пусть пространство X с объемом ℓ регулярно. Тогда существует оптимальный способ описания f объектов из $X \times \mathbb{N}_\perp$ с помощью объектов из X. Сравним его со способом g_n, сопоставляющим объекту x объект

$\langle x, n\rangle$. Так как f оптимален, то $K_f(\langle X\times \mathbb{N}_\perp, \{\langle x_0, n\rangle\}\rangle)$ превышает $K_{g_n}(\langle X\times \mathbb{N}_\perp, \{\langle x_0, n\rangle\}\rangle) = \ell(x_0)$ не более чем на константу (зависящую от n, но не зависящую от x).

Более сложно доказательство обратной импликации. Пусть $f\in C(X, X\times \mathbb{N}_\perp)$ - способ описания, удовлетворяющий условию $(*)$, Y - произвольное пространство. Согласно следствию предложения 1 из I.5, существует вычислимый объект $u\in C(X\times \mathbb{N}_\perp, Y)$, среди сечений $u_n : x\mapsto u(\langle x, n\rangle)$ которого встречаются все вычислимые объекты $C(X, Y)$. Рассмотрим теперь композицию $h = u\circ f : x\mapsto u(f(x))$. Согласно лемме 5 из I.5, она является вычислимым объектом пространства $C(X, Y)$, то есть способом описания объектов Y с помощью объектов пространства X. Докажем, что h - оптимальный способ описания. Пусть g - произвольный способ описания объектов Y с помощью объектов пространства X. Тогда $g(x) = u(\langle x, n\rangle)$ для некоторого n. По условию $(*)$ существует такое C, что для всех конечных $x_0\in X_0$ имеет место неравенство $K_f(\langle X\times \mathbb{N}_\perp, \{\langle x_0, n\rangle\}\rangle)\leq \ell(x_0)+C$. Пусть $\langle Y, A\rangle$ - произвольная задача в пространстве Y. Если $g(x_0)\in A$, то $u(\langle x_0, n\rangle)\in A$. Так как $K_f(\langle X\times \mathbb{N}_\perp, \{\langle x_0, n\rangle\}\rangle) < \ell(x_0)+C+1$, то существует конечный объект x_1 пространства X, для которого

$$f(x_1) = \langle x_0, n\rangle,\quad \ell(x_1) < \ell(x_0)+C+1.$$

Тогда $h(x_1) = u(f(x_1)) = u(\langle x_0, n\rangle) = g(x_0)\in A$. Таким образом, для всякого x_0, для которого $g(x_0)\in A$, мы нашли x_1, для которого $h(x_1)$ и $\ell(x_1) < \ell(x_0)+C+1$. Отсюда получаем, что $K_h(\langle Y, A\rangle)\leq K_g(\langle Y, A\rangle)+C+1$. Оптимальность h доказана. ▨

Пусть X - регулярное пространство с объемом, Y - любое пространство. Выберем и зафиксируем оптимальный способ описания

h объектов Y с помощью объектов X. Сложность задачи $\alpha = \langle Y, A \rangle$ при способе описания h мы будем называть энтропией задачи α. Произвол в выборе оптимального способа кодирования влечет за собой то, что энтропия определена с точностью до ограниченного слагаемого. Энтропию задачи α мы будем обозначать $K_{X,\ell}(\alpha)$ (здесь X - пространство описаний, ℓ - объем на нем) или просто $K_X(\alpha)$ или $K(\alpha)$, если ℓ и X ясны из контекста.[ж)]

Предложение 2. Пусть X, ℓ - произвольное регулярное пространство с объемом, $\alpha = \langle Y, A \rangle$ - произвольная задача. Тогда $K_{X,\ell}(\alpha) < \infty \Leftrightarrow \alpha$ разрешима.

Доказательство. Предложение следует из леммы I п. 2.2. ▨

Таким образом, мы расклассифицировали разрешимые задачи по степени трудность их решения, точнее, по степени трудности описания их решений с помощью объектов заданного пространства X с объемом ℓ.

ж) В дальнейшем мы будем часто использовать вольность речи, говоря "регулярное пространство X с объемом ℓ" или просто "регулярное пространство X" вместо "пространство X и объем ℓ на нем, превращающий X в регулярное пространство с объемом"

2.4. Примеры энтропий.

В этом пункте мы рассмотрим некоторые регулярные пространства с объемом. Каждому из них соотвествует свой вариант понятия энтропии.

2.4.I. Проверим, что пространство $\mathbb{N}_\perp$ с объемом ℓ : $\ell(\perp)=0,\ \ell(n)=\log_2(n+1)$ регулярно, и, следовательно, может служить для определения энтропии. Согласно предложению I из 2.3 достаточно построить такой способ f описания объектов $\mathbb{N}_\perp \times \mathbb{N}_\perp$ объектами $\mathbb{N}_\perp$, что

$$(\forall n \in \mathbb{N})(\exists c)(\forall m \in \mathbb{N}_\perp)(K_f(\langle \mathbb{N}_\perp \times \mathbb{N}_\perp, \{\langle m,n\rangle\}\rangle) \leq \ell(m)+c).$$

В качестве такового можно взять способ f, определяемый так: $f(k)=\langle m,n\rangle \Leftrightarrow k=2^n\cdot(2m+3)$ при $k, n \in \mathbb{N}$, $m \in \mathbb{N}_\perp$, где $2\perp+3$ полагаем равным 1, а $f(\perp)=$ $=\langle\perp,\perp\rangle$. Очевидно, $K_f(\langle \mathbb{N}_\perp \times \mathbb{N}_\perp, \{\langle m,n\rangle\}\rangle) \leq n+\log_2(2m+$ $+3) \leq \ell(m)+c(n)$.

2.4.2. Покажем, что пространство Ω с объемом ℓ: $\ell(x)$ =(длина последовательности x) является регулярным. Для этого нужно построить такой способ описания f объектов $\Omega \times \mathbb{N}_\perp$ объектами Ω, чтобы

$$(\forall n \in \mathbb{N})(\exists c)(\forall x \in \Omega)(K_f(\langle \Omega \times \mathbb{N}_\perp, \{\langle x,n\rangle\}\rangle) \leq \ell(x)+c).$$

В качестве f можно взять такой элемент пространства $C(\Omega, \Omega \times \mathbb{N}_\perp)$, что $f(0^n 1 x)=\langle x,n\rangle$ для всех $n \in \mathbb{N}$ и $x \in \Omega$, а $f(0^k)=\perp$. (Здесь 0^s обозначает слово из s нулей.) Очевидно, $K_f(\langle \Omega \times \mathbb{N}_\perp, \{\langle x,n\rangle\}\rangle) \leq n+\ell(x)+1$.

2.4.3. Покажем, что пространство Ξ с объемом ℓ: $\ell(x)$ = (число элементов в области определения x) регулярно. Для этого возьмем $f \in C(\Xi, \Xi \times \mathbb{N}_\perp)$, переводящий функцию x в пару (y, n), для которой

$x(0)=0,\ x(1),\ldots,\ x(n-1)=0,\ x(n)=1,\ y(i)\simeq x(n+i+1)$

при всех i (если такая существует) и в $(\perp,\perp)$, если пары с указанными свойствами не существует. Очевидно,

$$K_f(\langle \Xi \times \mathbb{N}_\perp, \{\langle y, n\rangle\}\rangle) \leq n + \ell(y) + 1.$$

2.5. Сравнение различных энтропий.

Пусть X_1, ℓ_1 и X_2, ℓ_2 - два регулярных пространства с объемом на них; мы хотим выяснить, как связаны энтропии $K_{X_1,\ell_1}(\alpha)$ и $K_{X_2,\ell_2}(\alpha)$ одной и той же задачи α при разных пространствах описаний. Более конкретно, нас интересует, в каких случаях имеются оценки вида

$$K_{X_1}(\alpha) \leq f(K_{X_2}(\alpha)) + C$$

где f - некоторая функция. Ответ на этот вопрос дает

Предложение I. Пусть $f: \mathbb{R} \to \mathbb{R}$ - монотонно возрастающая функция, удовлетворяющая условию Липшица. Тогда следующие свойства равносильны:

(I) Для любого пространства Y существует такое C, что для любой задачи $\alpha = \langle Y, A \rangle$ имеет место неравенство

$$K_{X_1,\ell_1}(\alpha) \leq f(K_{X_2,\ell_2}(\alpha)) + C.$$

(2) Существует такое C, что для всякого конечного объекта $x_2 \in X_2$ выполнено неравенство

$$K_{X_1,\ell_1}(\langle X_2, \{x_2\}\rangle) \leq f(\ell_2(x_2)) + C.$$

Доказательство. (I)$\Rightarrow$(2). Возьмем в качестве Y пространство X_2. Тогда существует такое C, что для любой задачи $\alpha = \langle Y, A \rangle$, в частности, для любой задачи вида $\langle X_2, \{x_2\}\rangle$ выполнено неравенство

$$K_{X_1,\ell_1}(\langle X_2, \{x_2\}\rangle) \leq f(K_{X_2,\ell_2}(\langle X_2, \{x_2\}\rangle)) + C.$$

Учитывая неравенство $K_{X_2,\ell_2}(\langle X_2, \{x_2\}\rangle) \leq \ell(x_2) + C'$, получаемое рассмотрением тождественного способа кодирования объектов X_2 с помощью объектов X_2, а также то, что функция f монотонна и удовлетворяет условию Липшица, имеем

$$K_{X_1,\ell_1}(\langle X_2, \{x_2\}\rangle) \leq f(\ell(x_2) + C') + C \leq$$
$$\leq f(\ell(x_2)) + C'' + C.$$

(2) $\Rightarrow$ (I). Пусть $t \in C(X_1, X_2)$ - оптимальный способ описания;

тогда $K_f(\langle X_2, \{x_2\}\rangle) \leq f(\ell_2(x_2)) + C.$

Пусть $g \in C(X_2, Y)$ - оптимальный способ описания объектов Y с помощью объектов из X_2. Рассмотрим способ описания $h = g \circ t$ объектов Y с помощью объектов из X_1. Пусть $\alpha = \langle Y, A\rangle$ - задача в пространстве Y, x_2 - конечный объект X_2, для которого $g(x_2) \in A$, $\ell(x_2) \leq K_{X_2,\ell_2}(\alpha) + 1$. Пусть x_1 - конечный объект X_1, для которого $t(x_1) = x_2$ и $\ell(x_1) \leq f(\ell_2(x_2)) + C + 1$. Тогда $h(x_1) = g(x_2) \in A$ и $K_h(\alpha) \leq \ell(x_1) \leq f(\ell_2(x_2)) + C + 1 \leq f(K_{X_2,\ell_2}(\alpha) + 1) + C + 1 \leq$ $\leq f(K_{X_2,\ell_2}(\alpha)) + C'$ (пользуемся монотонностью и условием Липшица). Поэтому и для оптимального способа кодирования верно аналогичное неравенство. ▨

Если мы интересуемся только энтропией монотонных задач, то условие (2) следует несколько видоизменить. Именно, справедливо следующее

Предложение 2. Пусть $f: \mathbb{R} \to \mathbb{R}$ - монотонно возрастающая функция, удовлетворяющая условию Липшица. Тогда следующие свойства равносильны:

(I') Для любого пространства Y существует такое C, что для любой монотонной задачи $\alpha = \langle Y, A\rangle$ имеет место неравенство $K_{X_1,\ell_1}(\alpha) \leq f(K_{X_2,\ell_2}(\alpha)) + C.$

(2') Существует такое C, что для всякого конечного объекта $x_2 \in X_2$ выполнено неравенство

$$K_{X_1,\ell_1}(\langle X_2, \Gamma_{x_2}\rangle) \leq f(\ell_2(x_2)) + C$$

(напомним, что $\Gamma_{x_2} = \{x \in X_2 \mid x \geq x_2\}$).

Доказательство. Чтобы доказать импликацию (I') ⇒ (2'), нужно внести в доказательство импликации (I') ⇒ (2) следующее изменение: всюду задача $\langle X_2, \{x_2\}\rangle$ заменяется на монотонную задачу $\langle X_2, \Gamma_{x_2}\rangle$. Доказательство (2') ⇒ (I') получается из доказательства импликации (2) ⇒ (I) предыдущего предложения

заменой $\langle X_2, \{x_2\}\rangle$ на $\langle X_2, \Gamma_{x_2}\rangle$, равенства $f(x_1)=x_2$ на неравенство $f(x_1)\geq x_2$ и равенства $h(x_1)=g(x_2)$ на неравенство $h(x_1)\geq g(x_2)$. ▨

Нас будут особенно интересовать случаи функций $f(n)=n$ и $f(n)=n+C\log_2 n$. Если выполнены условия (I′) и (2′) предложения 2 для функции $f(n)=n$, то мы будем говорить, что пространство X_1 не хуже пространства X_2. Если условия (I′) и (2′) предложения 2 выполнены для функции $f(n)=n+C\log_2 n$ при некотором C, то мы будем говорить, что пространство X_1 почти не хуже пространства X_2. Имеет место простая

Лемма I. Оптношения "X_1 не хуже X_2" и "X_1 почти не хуже X_2" транзитивны; выполнение первого из них влечет выполнение второго.

Доказательство очевидно, если воспользоваться условием (I′) предложения 2. ▨

Сравним с этой точки зрения введенные в 2.4 энтропии.

Предложение 3. Имеют место соотношения

$$\mathbb{N}_\perp \overset{\longleftarrow ---}{\longrightarrow} \Omega \longleftarrow \Xi$$

где $X\to Y$ означает, что X не хуже Y,

$X \dashrightarrow Y$ означает, что X почти не хуже Y;

иных соотношений (кроме вытекающих из указанных с помощью Леммы I) нет.

Доказательство. (I) $\mathbb{N}_\perp \to \Omega$. Рассмотрим следующий способ f описания объектов Ω с помощью объектов $\mathbb{N}_\perp$: $f(\perp)$ = пустое слово, $f(n)$ = двоичная запись числа $n+1$, у которой отброшена первая единица. Для него выполнено свойство (2′) из предложения 2 (и даже более сильное свойство (2) из предложения I).

(2) $\Xi \to \Omega$. Рассмотрим следующий способ f описания объектов Ω с помощью объектов Ξ:

$f(x) = x(0)\dots x(k)$, где k - наибольшее натуральное число, для которого $x(0), x(1), \dots, x(k)$ определены. (Если x - всюду определенная функция, то $f(x) = x(0)x(1)\dots$ - бесконечная последовательность.) Для построенного f выполнено свойство ($2'$) из предложения 2 и даже более сильное свойство (2) из предложения I.

(3) $\Omega \dashrightarrow \mathbb{N}_\perp$. Сопоставим каждому натуральному числу n двоичную последовательность x_n, причем так, чтобы $x_m \not\leq x_n$ при $m \neq n$ и $l(x_n) \leq \log_2 n + 2\log_2\log_2 n + C$. Это можно сделать, например, таким способом. Каждому числу n сопоставим сперва двоичную последовательность $\tilde{n}$, получающуюся из двоичной записи числа $n+1$ отбрасыванием первой единицы. Через $\overline{u}$ (где u - двоичная последовательность) обозначим последовательность, получающуюся из u заменой каждого нуля на 00 и каждой единицы на II. Теперь положим

$$x_n = \overline{(\text{длина } \tilde{n})}\,01\tilde{n}$$

В качестве искомого способа описания f элементов $\mathbb{N}_\perp$ с помощью элементов Ω возьмем точную верхнюю грань множества $\{(x_n \longmapsto n) \mid n \in \mathbb{N}\} \subset C(\Omega, \mathbb{N}_\perp)$. Очевидно, $K_f(n) \leq l(x_n) \leq l(n) + 2\log_2 l(n) + C$.

(4) Докажем теперь, что $\mathbb{N} \not\dashrightarrow \Xi$. В самом деле, пусть $\mathbb{N}_\perp$ почти не хуже Ξ и f - способ описания объектов Ξ с помощью объектов $\mathbb{N}_\perp$, для которого

$$K_f(\langle \Xi, \Gamma_x \rangle) \leq l_\Xi(x) + C_1 \log_2 l_\Xi(x) + C_2$$

Рассмотрим все функции $x \in \Xi$, область определения которых состоит из двух элементов; для каждой из них рассмотрим задачу Γ_x. Сложность этих задач (при способе описания f) должна быть ограничена некоторой константой C_3. Пусть $n_1, \dots, n_k$ - все те натуральные числа n, для которых $l(n) \leq C_3$. Для всякой функции x с двухэлементной областью

определения существует i , для которого $f(n_i) \in \Gamma_x$. Таким образом, мы получаем конечное число функций $x_1 = f(n_1)$, $\ldots, x_k = f(n_k)$ и каждая функция с двухэлементной областью определения является сужением одной из функций x_i . А это невозможно. В самом деле, будем говорить, что число a эквивалентно числу b , если для всех i выполнено условное равенство $x_i(a) \simeq x_i(b)$. Классов эквивалентности конечное число (не более 3^k), поэтому существуют различные, но эквивалентные числа a и b . Тогда функция x , для которой $x(a) = 0$, $x(b) = 1$, а значения в остальных точках не определены, не является сужением ни одной из функций x_i.

(5) Докажем, что $\Xi \not\to \mathbb{N}_\perp$. Для этого введем на Ξ меру μ , сосредоточенную на множестве всюду определенных функций и совпадающую там с равномерной мерой Лебега (произведением счетного числа мер μ_i на $\{0,1\}$, для каждой из которых $\mu_i(0) = \mu_i(1) = 1/2$). Пусть f – способ описания элементов $\mathbb{N}_\perp$ с помощью элементов Ξ . Сопоставим каждому числу $n \in \mathbb{N}$ меру p_n множества $f^{-1}(\Gamma_n)$: $p_n = \mu(f^{-1}(\Gamma_n))$. Если $f(x) = n$, то $f^{-1}(\Gamma_n)$ содержит все продолжения x , поэтому $p_n \geq 2^{-\ell(x)}$. Таким образом $p_n \geq 2^{-K_f(\Gamma_n)}$. Если бы $K_f(\Gamma_n)$ было меньше $\ell(n) + C$, то было бы выполнено неравенство $p_n \geq 2^{-(\ell(n)+C)} \geq \frac{c_1}{n}$ и ряд $\sum p_i$ расходился бы. Но множества $f^{-1}(\Gamma_n)$ не пересекаются, а потому $\sum p_i \leq 1$. Полученное противоречие показывает, что $\Xi \not\to \mathbb{N}_\perp$.

Предложение 3 доказано. ▨

2.6. Сравнение энтропий различных задач.

В этом пункте мы докажем неравенство, связывающее энтропию различных задач при одном и том же пространстве описаний (в отличие от предыдущего пункта, где сравнивались энтропии одной и той же задачи при разных пространствах описаний).

Предложение I. Пусть X, ℓ – регулярное пространство с объемом, Y, Z – пространства, F – вычислимый объект пространства $C(Y, Z)$. Тогда существует такая константа C, что для любых задач $\alpha = \langle Y, A \rangle$ и $\beta = \langle Z, B \rangle$, для которых $F(A) \subset B$, имеет место неравенство

$$K_{X,\ell}(\beta) \leq K_{X,\ell}(\alpha) + C.$$

Заметим, что условие $F(A) \subset B$ можно переформулировать так: $A \subset F^{-1}(B)$.

Доказательство. Пусть $h \in C(X, Y)$ – оптимальный способ описания. Рассмотрим способ описания $F \circ h$ объектов Z объектами X. Тогда, очевидно, имеет место неравенство $K_{F \circ h}(\beta) \leq K_h(\alpha)$, откуда и вытекает нужное нам утверждение. ▨

Это предложение мы неоднократно будем использовать в дальнейшем. Отметим также такое очевидное свойство: если $\alpha = \langle Y, A \rangle$ и $\beta = \langle Y, B \rangle$ – две задачи в одном и том же пространстве и $A > B$, то $K_{X,\ell}(\alpha) \leq K_{X,\ell}(\beta)$ для любого регулярного пространства с объемом X, ℓ.

Глава 3. Задачи и интуиционистская логика.

В этой главе мы определим логические операции над задачами, покажем, что задачи образуют модель интуиционистской логики высказываний и выведем из этого некоторые следствия, касающиеся энтропии задач.

3.1. Логические операции над задачами.

В этом пункте мы определим (в духе идей А.Н.Колмогорова [18], развитых впоследствии Ю.Т.Медведевым [9]) логические операции над задачами.

Пусть $\alpha = \langle X, A\rangle$ и $\beta = \langle Y, B\rangle$ - две задачи. Конъюнкцией задач α и β назовем задачу

$$\alpha \wedge \beta = \langle X \times Y, A \times B\rangle$$

Дизъюнкцией задач α и β называется задача $\alpha \vee \beta = \langle X+Y, A' \cup B'\rangle$, где $A' = A$ и $B' = B$, если пространства X и Y не пересекаются; если это не так и при определении суммы пространства X и Y заменены на изоморфные непересекающиеся пространства X' и Y', то множества A' и B' - образы множеств A и B при изоморфизмах.

Импликацией задач α и β назовем задачу

$$\alpha \supset \beta = \langle C(X,Y), \{f \mid f(A) \subset B\}$$

Ложью (стандартной неразрешимой задачей) назовем задачу $F = \langle P, \emptyset\rangle$, где P - одноэлементное пространство, описанное в 1.2.1.

Таким образом, решить задачу $\alpha \wedge \beta$ означает предъявить пару $\langle$ решение задачи α, решение задачи $\beta \rangle$; решить задачу $\alpha \vee \beta$ означает указать, какая из задач α и β решается и затем предъявить ее решение; решить задачу $\alpha \supset \beta$ означает предъявить (непрерывную) функцию из пространства задачи α в пространство задачи β, перерабатывающую любое решение задачи α в некоторое решение задачи β.

Предложенные определения сходны по замыслу с определениями операций над финитными задачами, данными Медведевым в [9].

Различие состоит в том, что мы рассматриваем не просто множества без всякой структуры на них, а пространства; в частности, в определении задачи $\alpha \supset \beta$ участвуют непрерывные функции.

Для нас эта конструкция важна как общий метод доказательства неравенств, связанных с энтропией; об этом см. далее, в 3.4.

3.2. Энтропия конъюнкции, дизюнкции и импликации задач.

В этом пункте мы рассмотрим, как связаны энтропии конъюнкции, дизъюнкции и импликации с энтропиями исходных задач.

3.2.I. Конъюнкция.

Для рассмотрения энтропии конъюнкции двух задач нам понадобится следующая вспомогательная конструкция.

Пусть X, Y – два пространства с введенными на них объемами ℓ_X, ℓ_Y, являющихся регулярными. Введем в пространстве $X\times Y$ объем, положив

$$\ell_{X\times Y}(\langle x_0, y_0\rangle) = \ell_X(x_0) + \ell_Y(y_0).$$

(Свойства объема, перечисленные в I.6, очевидно выполнены.)

Лемма I. Пространство $X\times Y$ с объемом $\ell_{X\times Y}$ является регулярным.

Доказательство. Нам нужно построить такой способ описания $f\in C(X\times Y, X\times Y\times \mathbb{N}_\perp)$, что (*)

$$(\forall n\in\mathbb{N})(\exists c)(\forall x_0\in X_0)(\forall y_0\in Y_0)(K_f(\langle X\times Y\times\mathbb{N}_\perp, \{\langle x_0,y_0,n\rangle\}\rangle)\le \ell(x_0)+\ell(y_0)+c)$$

(Здесь X_0, Y_0 – множества конечных объектов пространств X и Y.) Для этого рассмотрим способ описания $g\in C(Y, Y\times\mathbb{N}_\perp)$, удовлетворяющий свойству

$$(\forall n\in\mathbb{N})(\exists c)(\forall y_0\in Y_0)(K_f(\langle Y\times\mathbb{N}_\perp, \{\langle y_0,n\rangle\}\rangle)\le \ell(y_0)+c) \quad (**)$$

и в качестве f возьмем отображение, определяемое так: $f(x,y) = (x, g(y))$. Докажем, что свойство $(*)$ выполнено. Пусть $n\in\mathbb{N}$. Соответствующее этому n значение c, для которого неравенство $(**)$ выполнено, обозначим c_1. Пусть $x_0\in X_0$, $y_0\in Y_0$. Если $g(y_1)=\langle y_0, n\rangle$, $y_1\in Y_0$, то $f(x_0,y_1)=\langle x_0,y_0,n\rangle$, поэтому

$$K_f(\langle X\times Y\times\mathbb{N}_\perp, \{\langle x_0,y_0,n\rangle\}\rangle)\le \ell_{X\times Y}(\langle x_0,y_1\rangle) = \ell_X(x_0)+\ell_Y(y_1).$$

В силу указанного свойства способа описания g при данном y_0 можно выбрать y_1 так, чтобы $g(y_1)=\langle y_0, n\rangle$ и

и $l_Y(y_1) \leq l_Y(y_0) + C_1 + 1$. Тогда $l_X(x_0) + l_Y(y_1) \leq$
$\leq l_X(x_0) + l_Y(y_0) + C_1 + 1$ Поэтому условие (*) выполнено.

Эта лемма позволяет сформулировать

<u>Предложение I</u>. Пусть M, N – два пространства, X и Y – два регулярных пространства с объемами l_X и l_Y. Тогда существует такая константа C, что для всех задач α в пространстве M и для всех задач β в пространстве N выполнено неравенство

$$K_{X\times Y, l_{X\times Y}}(\alpha \wedge \beta) \leq K_{X, l_X}(\alpha) + K_{Y, l_Y}(\beta) + C.$$

Это предложение утверждает, что сложность решения конъюнкции двух задач (т.е. сложность их одновременного решения) не превосходит суммы сложностей исходных задач (при подходящем выборе пространства описаний).

<u>Доказательство</u>. Пусть $\alpha = \langle M, A\rangle$, $\beta = \langle N, B\rangle$, f – оптимальный способ описания объектов из M объектами X, g – оптимальный способ описания объектов из N объектами Y. Рассмотрим способ описания $h \in C(X\times Y, M\times N)$ определенный формулой $h(x,y) = \langle f(x), g(y)\rangle$

Докажем, что $K_h(\alpha \wedge \beta) \leq K_f(\alpha) + K_g(\beta)$.
(Отсюда будет следовать интересующее нас утверждение.)
В самом деле, если $f(x_0) \in A$, $g(y_0) \in B$, то $h(x_0, y_0) \in$
$\in A\times B$ и $K_h(\alpha \wedge \beta) \leq l_{X\times Y}(\langle x_0, y_0\rangle) = l_X(x_0) + l_Y(y_0)$
Беря точную нижнюю грань по всем x_0 и y_0, получаем требуемое неравенство.

Из предложения I вытекает такое полезное

<u>Следствие I предложения I</u>. Пусть X – такое регулярное пространство с объемом, что X не хуже $X \times X$. Тогда для всяких пространств M и N найдется такое C, что для любых задач α и β в пространствах M и N соответственно выполнено неравенство $K_X(\alpha \wedge \beta) \leq K_X(\alpha) + K_X(\beta) + C$. ▨

В качестве пространства X, удовлетворяющего указанному требованию, можно взять, например, пространство Ξ, как показывает следующая

Лемма 2. Ξ не хуже $\Xi \times \Xi$.

Доказательство. Определим способ описания $f \in C(\Xi, \Xi \times \Xi)$ формулой

$$f(x) = \langle y, z \rangle \Leftrightarrow \forall n \, (y(n) \simeq x(2n) \,\&\, z(n) \simeq x(2n+1)).$$

Ясно, что $K_f^{\langle \Xi \times \Xi, 1 \rangle}(\langle y_0, z_0 \rangle) \leq \ell(y_0) + \ell(z_0)$. Остается воспользоваться предложением 2 из 2.5. ▨

Пространство $\mathbb{N}_\perp$ не обладает аналогичным свойством – не существует способа описания $f \in C(\mathbb{N}_\perp, \mathbb{N}_\perp \times \mathbb{N}_\perp)$ и константы C, для которых $K_f(\langle m, n \rangle) \leq \ell(m) + \ell(n) + C$ при всех $m, n \in \mathbb{N}_\perp$. В самом деле, для любого числа A количество тех пар $\langle m, n \rangle$, для которых $K_f(\langle m, n \rangle) \leq A + C$, не превосходит $C_1 \cdot 2^A$, а количество тех пар $\langle m, n \rangle$, для которых $\ell(m) + \ell(n) \leq A$, при больших A становится больше $C_1 \cdot 2^A$.

Однако верна такая

Лемма 3. $\mathbb{N}_\perp$ почти не хуже $\mathbb{N}_\perp \times \mathbb{N}_\perp$.

Доказательство. Пусть $\varphi : \mathbb{N}^2 \to \mathbb{N}$ – всюду определенное инъективное отображение, для которого

$$\ell(\varphi(m, n)) \leq \ell(m) + \ell(n) + 2 \log \ell(m) + C$$

при всех m и n и подходящей константе C. Построить такое φ можно, например, следующим образом. Сопоставим каждому числу u слово $\overline{u}$ в алфавите $\{0, I\}$, получающееся из двоичной записи числа $1+u$ отбрасыванием первой единицы. Через $\tilde{v}$ обозначим слово, получающееся из слова v удвоением каждой буквы (заменой 0 на 00 и I на II). Теперь определим функцию φ так, чтобы $\overline{\varphi(m,n)} = \widetilde{\overline{\ell(m)}}\, 01\, \overline{u}\, \overline{v}$

После того, как функция φ с указанным свойством по-

строена, мы можем определить способ кодирования $f \in C(\mathbb{N}_\perp, \mathbb{N}_\perp \times \mathbb{N}_\perp)$ так: $f(\perp) = \langle \perp, \perp \rangle$, $f(n) = \langle \perp, k \rangle$, если $\varphi(0, k+1) = n$, $f(n) = \langle k, \perp \rangle$, если $\varphi(k+1, 0) = n$, $f(n) = \langle k, l \rangle$, если $\varphi(k+1, l+1) = n$. Ясно, что

$$K_f(\mathbb{N}_\perp \times \mathbb{N}_\perp, \{\langle m, n \rangle\}) \le l(m) + l(n) + 2\log l(n) + c.$$

Остается воспользоваться предложением 2 из 2.5. ▨

Лемма 3 позволяет применить к случаю $X = \mathbb{N}_\perp$ такое

Следствие 2 предложения I. Пусть X – такое регулярное пространство, что X почти не хуже $X \times X$. Тогда для всяких пространств M и N найдутся такие c_1 и c_2, что для всяких задач α и β в пространствах M и N соответственно выполнено неравенство

$$K_X(\alpha \wedge \beta) \le K_X(\alpha) + K_X(\beta) + c_1 \log(K_X(\alpha) + K_X(\beta)) + c_2. \text{ ▨}$$

3.2.2. Дизъюнкция.

Если для случая конъюнкции мы имели лишь неравенство, ограничивающее сверху энтропию $\alpha \wedge \beta$, то энтропия дизъюнкции $\alpha \vee \beta$ задач α и β определяется энтропиями исходных задач. Точную формулировку этого утверждения дает

Предложение 2. Пусть X – регулярное пространство, M, N – два пространства. Тогда существует такая константа C, что для любых задач α и β в пространствах M и N соответственно имеет место неравенство

$$|K_X(\alpha \vee \beta) - \min(K_X(\alpha), K_X(\beta))| \le C.$$

Это предложение показывает, что дизъюнкцию задач α и β решить так же трудно (с точностью до ограниченного слагаемого), как решить более легкую из задач α и β.

Доказательство. Докажем, что существует C, для которого $K_X(\alpha \vee \beta) \le K_X(\alpha) + C$. В самом деле, пусть $f \in C(X, M)$ – оптимальный способ описания. Рассмотрим

способ описания $g \in C(X, M+N)$, являющийся композицией $i \circ f$ отображения f с отображением вложения $i \in C(M, M+N)$. Очевидно, $K_g(\alpha \vee \beta) \le K_f(\alpha)$, откуда и следует указанное неравенство.

Аналогично получаем, что $K_X(\alpha \vee \beta) \le K_X(\beta) + c'$.

Осталось доказать, что

$$\min(K_X(\alpha), K_X(\beta)) \lesssim K_X(\alpha \vee \beta) + c''$$

Пусть $f \in C(X, M+N)$ - оптимальный способ описания. Построим способы описания $g \in C(X, M)$ и $h \in C(X, N)$ следующим образом:

$$g(x) = \begin{cases} \bot_M & \text{, если } f(x) = \bot_{M+N} \text{ или } f(x) \in N \\ f(x) & \text{, если } f(x) \in M \end{cases}$$

$$h(x) = \begin{cases} \bot_N & \text{, если } f(x) = \bot_{M+N} \text{ или } f(x) \in M \\ f(x) & \text{, если } f(x) \in N \end{cases}$$

Очевидно, $K_f(\alpha \vee \beta) = \min(K_g(\alpha), K_h(\beta))$ откуда и вытекает требуемое неравенство. ☒

3.2.3. Импликация

Пусть α и β - задачи. Назовем энтропию задачи $\alpha \supset \beta$ условной энтропией задачи β при известной α. Ее иногда мы будем обозначать также $K(\beta | \alpha)$. Величина $K(\beta | \alpha)$ показывает, насколько трудно решить задачу β в предположении, что решение задачи α известно.

Обсуждение свойств условной энтропии мы отложим до п. 3.4, где будут доказаны некоторые связанные с ней неравенства.

3.3. Задачи образуют модель интуиционистского исчисления высказываний.

Пусть $\Phi(p_1, \dots, p_n)$ - пропозициональная формула в языке, содержащем $\wedge$, $\vee$, $\supset$ и F (ложь). Если вместо переменных $p_1, \dots, p_n$ подставить задачи $\alpha_1, \dots, \alpha_n$ и понимать $\wedge$, $\vee$, $\supset$ и F в описанном смысле как операции над задачами, то возникнет некоторая задача, которую естественно обозначить $\Phi(\alpha_1, \dots, \alpha_n)$. Оказывается, что эта задача всегда разрешима и, более того, ее энтропия ограничена константой, не зависящей от выбора задач $\alpha_1, \dots, \alpha_n$. Прежде чем сформулировать точно это утверждение, дадим некоторые пояснения.

Пусть $\Phi(p_1, \dots, p_n)$ - формула, $\alpha_1 = \langle X_1, A_1 \rangle, \dots, \alpha_n = \langle X_n, A_n \rangle$ - задачи. Заметим, что пространство задачи $\Phi(\alpha_1, \dots, \alpha_n)$ определяется пространствами $X_1, \dots, X_n$ и не зависит от выбора множеств $A_1, \dots, A_n$. Поэтому мы можем корректно обозначить его $\Phi(X_1, \dots, X_n)$

Теорема. Пусть $\Phi(p_1, \dots, p_n)$ - выводимая формула интуиционистского исчисления высказываний, $X_1, \dots, X_n$ - пространства. Тогда существует вычислимый объект в пространстве $\Phi(X_1, \dots, X_n)$, являющийся решением задачи $\Phi(\langle X_1, A_1 \rangle, \dots, \langle X_n, A_n \rangle)$ при любых $A_i \subset X_i$.

Следствие. Энтропия задач $\Phi(\langle X_1, A_1 \rangle, \dots, \langle X_n, A_n \rangle)$ (при любом выборе пространства описаний) ограничена константой, зависящей только от пространств X_i и пространства описаний (и не зависящей от выбора A_i). ▨

Эта теорема даст нам также возможность (в 3.4) единым образом доказать ряд неравенств для энтропии.

Доказательство теоремы ведется индукцией по выводу формулы. Технически удобнее рассматривать интуиционистское исчисление высказываний в форме, приведенной в книге А.Г. Драгалина [3] под названием пропозиционального фрагмента HPC_1 (схемы аксиом и правила вывода I – II на с. 2I). Эта формулировка состоит из следующих схем аксиом и правил вывода:

I) $\dfrac{\varphi \quad \varphi \supset \psi}{\psi}$ 2) $\dfrac{\varphi \supset \psi \quad \psi \supset \eta}{\varphi \supset \eta}$

3) $\dfrac{\varphi \wedge \psi \supset \eta}{\varphi \supset (\psi \supset \eta)}$ 4) $\dfrac{\varphi \supset (\psi \supset \eta)}{\varphi \wedge \psi \supset \eta}$

5) $\varphi \wedge \psi \supset \varphi$ 6) $\varphi \wedge \psi \supset \psi \wedge \varphi$

7) $\varphi \supset \varphi \wedge \varphi$ 8) $\dfrac{\varphi \supset \eta \quad \psi \supset \eta}{\varphi \vee \psi \supset \eta}$

9) $\varphi \supset \varphi \vee \psi$ I0) $\varphi \vee \psi \supset \psi \wedge \varphi$

II) $F \supset \varphi$

Нам надо проверить, что для каждой аксиомы выполнено утверждение доказываемой теоремы и что если оно выполнено для посылок правила вывода, то оно выполнено и для его заключения. Эта проверка происходит довольно просто; тем не менее наметим ее.

I) Если объект a – постоянное вычислимое решение задачи $\varphi \supset \psi$, а объект b – постоянное вычислимое решение задачи φ, то результат применения a к b является постоянным решением задачи ψ. Его вычислимость обеспечивается леммой 3 из п. I.5. (Указания на то, в каких пространствах лежат рассматриваемые объекты, мы опускаем, так как они очевидно восстанавливаются.)

2) Если объект a – постоянное вычислимое решение задачи $\varphi \supset \psi$, а b – постоянное вычислимое решение задачи $\psi \supset \eta$, то $b \circ a$ – постоянное вычислимое решение зада-

чи $\varphi \supset \eta$ (Его вычислимость гарантируется леммой 5 из I.5.)

3) Применяем к постоянному вычислимому решению задачи $\varphi \wedge \psi \supset \eta$ стандартный изоморфизм $C(X \times Y, Z) \to$ $\to C(X, C(Y, Z))$, описанный в п. I.4.4.

4) Аналогично предыдущему пункту с заменой изоморфизма на обратный.

5) Искомым вычислимым решением является отображение проекции $f: X \times Y \to X$, определенное формулой $f(x, y) = x$.

6) Искомым вычислимым решением является отображение $f: X \times Y \to Y \times X$, определенное формулой

$$f(x, y) = \langle y, x \rangle$$

7) Искомым вычислимым решением является отображение $f: X \to X \times X$, определенное формулой $f(x) = \langle x, x \rangle$.

8) Этот пункт несколько сложнее предыдущих. Пусть X, Y, Z - пространства задач φ, ψ, η, $a \in C(X, Z)$ - постоянное вычислимое решение задачи $\varphi \supset \eta$, $b \in C(Y, Z)$ - постоянное вычислимое решение задачи $\psi \supset \eta$. Построим $c \in C(X+Y, Z)$ следующим образом:

$$c(t) = \begin{cases} \bot_Z, & \text{если } t = \bot_{X+Y} \\ a(t), & \text{если } t \in X \\ b(t), & \text{если } t \in Y \end{cases}$$

(Мы предполагаем, что X и Y не пересекаются; если это не так, следует внести очевидные изменения в определение c.) Очевидно, c является непрерывной функцией и, более того, вычислимым объектом пространства $C(X+Y, Z)$. Это c и будет решением задачи $\varphi \vee \psi \supset \eta$

9) Решением является стандартное вложение X в $X+Y$.

10) Решением является очевидный изоморфизм $X+Y \to Y+X$.

11) Решением является объект $(\bot \to \bot)$.

Теорема доказана.

Отметим, что, очевидно, в условиях теоремы нельзя заменить интуиционистское исчисление высказываний на классическое: формула $\neg\neg\varphi \supset \varphi$ не обладает указанным в теореме свойством ($\neg\alpha$ - сокращение для $\alpha \supset F$).

3.4. Неравенства для энтропии.

В этом пункте мы выведем из теоремы п. 3.3 некоторые следствия, касающиеся энтропии.

Предложение I. Пусть $\Phi(p_1,\dots,p_n) \supset \Psi(p_1,\dots,p_n)$ выводимая формула интуиционистского исчисления высказываний, $X_1,\dots, X_n$ - пространства, X - регулярное пространство с объемом. Тогда существует такое C, что для любых задач $\alpha_1 = \langle X_1, A_1\rangle,\dots,\alpha_n = \langle X_n, A_n\rangle$ выполнено неравенство

$$K_X(\Psi(\alpha_1,\dots,\alpha_n)) \leq K_X(\Phi(\alpha_1,\dots,\alpha_n)) + C.$$

Доказательство. Согласно теореме п. 3.3 существует вычислимый объект $f \in C(\Phi(X_1,\dots,X_n), \Psi(X_1,\dots,X_n))$ который переводит любое решение задачи $\Phi(\alpha_1,\dots,\alpha_n)$ в некоторое решение задачи $\Psi(\alpha_1,\dots,\alpha_n)$ (при любых $A_1,\dots, A_n$). Остается воспользоваться предложением I из п. 2.5. ▨

Следствие. Пусть X - регулярное пространство с объемом, M, N - пространства. Тогда существует такая константа C, что для любых задач $\alpha = \langle M, A\rangle$, $\beta = \langle N, B\rangle$ имеют место неравенства

(I) $K_X(\alpha) \leq K_X(\alpha\wedge\beta) + C$

(2) $K_X(\beta) \leq K_X(\alpha\wedge\beta) + C$

(3) $K_X(\alpha\supset\beta) \leq K_X(\beta) + C$

(4) $K_X(\beta) \leq K_X(\alpha\wedge(\alpha\supset\beta)) + C$

(5) $K_X(\alpha \mid \beta\supset\alpha) \leq K_X(\beta)$

(6) $K_X(\alpha\wedge\beta \mid \alpha) \leq K_X(\beta)$

Доказательство. В самом деле, в интуиционистском исчислении высказываний выводимы формулы $\varphi\wedge\psi\supset\varphi$, $\varphi\wedge\psi\supset\psi$, $\varphi\supset(\psi\supset\varphi)$, $\varphi\wedge(\varphi\supset\psi)\supset\psi$, $\varphi\supset((\varphi\supset\psi)\supset\psi)$, $\varphi\supset(\psi\supset(\varphi\wedge\psi))$. ▨

Приведенный список неравенств можно продолжить, взяв другие выводимые формулы, имеющие вид импликации.

3.5. Логика задач.

Рассмотрим множество Q пропозициональных формул, для которых справедливо утверждение теоремы п. 3.3. Эта теорема утверждает, что множество H выводимых в интуиционистском исчислении высказываний формул является частью Q. При доказательстве теоремы п. 3.3 было установлено также, что Q замкнуто относительно правила *modus ponens*. Очевидно, Q замкнуто и относительно правила подстановки и, следовательно, является суперинтуиционистской логикой. Так как $F \notin Q$, то эта логика непротиворечива, и, следовательно, является частью классического исчисления высказываний. Если обозначить множество тавтологий (=выводимых в классическом исчислении высказываний формул) через C, то можно записать: $H \subset Q \subset C$. Как отмечалось в 3.3, второе из этих включений - строгое. Следующее предложение показывает, что первое из них - также строгое.

Предложение I. $H \neq Q$.

Доказательство. Рассмотрим следующую"формулу Дж. Роуза": $R = ((\neg\neg\varphi \supset \varphi) \supset (\neg\varphi \vee \neg\neg\varphi)) \supset (\neg\varphi \vee \neg\neg\varphi)$, где $\varphi = \neg p \vee \neg q$. (Напоминаем, что $\neg\alpha$ есть сокращение для $\alpha \supset F$.) Как известно (см., например, [IO] ,с. I43), $R \notin H$. Докажем, что $R \in Q$. Заметим, что каково бы ни было пространство задачи α, пространство задачи $\neg\alpha$ одноэлементно, так как $C(X, P)$ изоморфно P (P - пространство из одного объекта $\perp$, см. I.2.I). Задача $\neg\alpha$ есть $\langle P, \emptyset \rangle$, если α непуста (имеет хоть одно решение) и есть $\langle P, P \rangle$, если α пуста (не имеет решений). Пространство задачи $\neg\alpha \vee \neg\beta$ имеет вид (изоморфно пространству $P + P$);

объект a (соответственно b) является ее решением тогда и только тогда, когда задача α (соответственно β) непуста.

Пространство задачи $\neg\neg\varphi \supset \varphi$ изоморфно пространству задачи φ , так как пространство задачи $\neg\neg\varphi$ одноэлементное. Отождествляя их, можно сказать, что решениями задачи $\neg\neg\varphi \supset \varphi$ являются все объекты пространства задачи φ , если φ пуста, или решения φ , если φ непуста.

Пусть $S = (\neg\neg\varphi \supset \varphi) \supset (\neg\varphi \vee \neg\neg\varphi)$ Объектами пространства задачи S являются непрерывные функции из пространства задачи $\neg\neg\varphi \supset \varphi$, отождествленного нами с пространством задачи φ , в пространство задачи $\neg\varphi \vee \neg\neg\varphi$ имеющее вид ⟶ (a, b над $\perp$)

Функция t является решением задачи S , если она:

(I) переводит все решения задачи φ в b , если задача φ непуста;

(2) переводит любой объект пространства задачи φ в a , если задача φ пуста.

Построим функцию f из пространства задачи S в пространство задачи $\neg\varphi \vee \neg\neg\varphi$ (имеющее вид ⟶ (a, b над $\perp$))

Именно,

$$f(t) = \begin{cases} a \text{, если значение функции } t \text{ на всех объектах равно } a; \\ b \text{, если значение функции } t \text{ хоть на одном объекте равно } b; \\ \perp \text{, если не имеет места ни один из указанных случаев.} \end{cases}$$

Легко видеть, что какова бы ни была задача φ , функция f переводит любое решение задачи S в решение задачи $\neg\varphi \vee \neg\neg\varphi$. Таким образом, f является решением задачи

если является непрерывной. (Это может быть и не так, если пространство задачи φ бесконечно). Однако поскольку в формуле R в качестве φ взято $\neg p \vee \neg q$, то, как легко видеть, f действительно является непрерывной и, более того, является вычислимым объектом пространства задачи R, какие бы пространства мы не взяли в качестве пространств задач p и q. Предложение доказано. $\boxtimes$

Формула R была предложена Дж.Роузом [19] как пример реализуемой в смысле С.К.Клини [6], но невыводимой формулы. Любопытно отметить, что другой пример реализуемой, но невыводимой формулы – "формула Цейтина", имеющая вид

$$((\neg p_1 \supset q_1 \vee q_2) \,\&\, (\neg p_2 \supset q_1 \vee q_2) \,\&\, \neg(p_1 \wedge p_2)) \supset$$
$$((\neg p_1 \supset q_1) \vee (\neg p_1 \supset q_2) \vee (\neg p_2 \supset q_1) \vee (\neg p_2 \supset q_2)),$$

– не принадлежит Q. Это показывает, что Q отличается от логики финитных задач Медведева [9] (которая содержит эту формулу).

4.I. Различные алгоритмические варианты понятия энтропии конечных объектов как частные случаи нашей схемы.

В этом пункте мы покажем, как различные рассматривавшиеся алгоритмические варианты понятия энтропии могут быть получены по нашей схеме с помощью подходящего выбора пространств объектов и описаний.

4.I.I. Простая колмогоровская энтропия

Пусть $X = \mathbb{N}_\perp, Y = \mathbb{N}_\perp$. Рассмотрим X со стандартным объемом (п. I.6) как пространство описаний и рассмотрим функцию

$$K(n) = K_X(\Gamma_n)$$

(В данном случае $\Gamma_n = \{n\}$)

Предложение I. $K(n)$ совпадает со сложностью n в смысле А.Н.Колмогорова [7]

И сложность по Колмогорову, и K определены с точностью до ограниченного слагаемого, поэтому, говоря о их совпадении, мы имеем в виду совпадение с указанной точностью.

Доказательство. Рассмотрим, какие возможны способы описания объектов $\mathbb{N}_\perp$ с помощью объектов $\mathbb{N}_\perp$. Пусть $f \in C(\mathbb{N}_\perp, \mathbb{N}_\perp)$. Если $f(\perp) = n \in \mathbb{N}$, то $f(x) = n$ для всех $x \in \mathbb{N}_\perp$. Если же $f(\perp) = \perp$, то функция $x \mapsto f(x)$ (при $x \in \mathbb{N}$) представляет собой частично рекурсивную функцию, доопределенную значением $\perp$ там, где она первоначально была не определена. Эта функция может быть любой частично рекурсивной функцией. После этих замечаний (и знакомства с определением Колмогорова) предложение I становится очевидным. ▨

4.I.2. Условная колмогоровская энтропия.

В работе [7] А.Н.Колмогоров определил также понятие условной энтропии (сложности) числа x при известном числе y, обозначаемой $K(x/y)$.

Предложение 2. $K(x,y) \asymp K_{\mathbb{N}_\perp}(\langle \mathbb{N}, \Gamma_y\rangle \supset \langle \mathbb{N}, \Gamma_x\rangle)$ (здесь $\langle \mathbb{N}_\perp, \Gamma_x\rangle$, $\langle \mathbb{N}_\perp, \Gamma_y\rangle$ - задачи в пространстве $\mathbb{N}_\perp$,*) их импликация - задача в пространстве $C(\mathbb{N}_\perp, \mathbb{N}_\perp)$; знак $\asymp$ означает сопадение с точностью до ограниченного слагаемого, см. замечание к предложению I.)

Доказательство. Прежде всего напомним колмогоровское определение величины $K(x/y)$, стоящей в левой части доказываемого равенства.

Пусть G - частично рекурсивная функция из $\mathbb{N}^2$ в $\mathbb{N}$. Колмогоров определяет $K_G(x/y)$ по формуле

$$K_G(x/y) = \inf\{\log_2(t+1) \mid G(t,y) = x\}$$

(некоторые несущественные технические различия мы не оговариваем). Среди всех функций G существует такая, для которой K_G минимально (для всякой G' существует такое C, что $K_G \le K_{G'} + C$). Функция K_G для одной из таких G и называется условной энтропией.

А. Покажем, что при подходящем C

$$K(x/y) \le K_{\mathbb{N}_\perp}(\Gamma_y \supset \Gamma_x) + C \qquad (*)$$

для любых x и y. Пусть $f \in C(\mathbb{N}_\perp, C(\mathbb{N}_\perp, C_{\mathbb{N}_\perp}))$ - оптимальный способ описания. Рассмотрим его образ $\tilde{f}$ при стандартном изоморфизме

$$C(\mathbb{N}_\perp, C(\mathbb{N}_\perp, \mathbb{N}_\perp)) \simeq C(\mathbb{N}_\perp \times \mathbb{N}_\perp, \mathbb{N}_\perp)$$

Очевидно, для любых t, x, y имеет место эквива-

*) Мы будем вместо $\langle \mathbb{N}, \Gamma_x\rangle$ и $\langle \mathbb{N}, \Gamma_y\rangle$ коротко писать Γ_x и Γ_y.

лентность

$$f(t) \in (\Gamma_y \supset \Gamma_x) \Leftrightarrow \tilde{f}(t,y) = x$$

При определении $K_f(\Gamma_y \supset \Gamma_x)$ можно не рассматривать $\perp$ в качестве описания (так как если $f(\perp) \in \Gamma_y \supset \Gamma_x$, то и $f(0) \in \Gamma_y \supset \Gamma_x$ и $\ell(\perp) = \ell(0)$). Определим частично рекурсивную функцию $\tilde{\tilde{f}}$ из $\mathbb{N}^2$ в $\mathbb{N}$, положив

$$\tilde{\tilde{f}}(t,y) = \begin{cases} \tilde{f}(t,y), & \text{если } \tilde{f}(t,y) \in \mathbb{N} \\ \text{не определено, если } \tilde{f}(t,y) = \perp \end{cases}$$

С учетом сделанных замечаний получаем, что

$K_{\tilde{\tilde{f}}}(x/y) = K_f(\Gamma_y \supset \Gamma_x)$, откуда и вытекает (ж).

Б. Покажем, что при подходящем C для всех x и y выполнено неравенство

$$K_{\mathbb{N}_\perp}(\Gamma_y \supset \Gamma_x) \leq K(x/y) + C$$

Пусть G функция, для которой $K_G(x/y)$ минимально. Рассмотрим функцию $g: \mathbb{N}_\perp \times \mathbb{N}_\perp \to \mathbb{N}_\perp$, определенную формулой

$$g(x,y) = \begin{cases} \perp, \text{ если } x = \perp \text{ или } y = \perp \\ G(x,y), \text{ если } x,y \in \mathbb{N} \text{ и } G(x,y) \text{ определено} \\ \perp, \text{ если } x,y \in \mathbb{N} \text{ и } G(x,y) \text{ не определено} \end{cases}$$

Функция g является вычислимым объектом пространства $C(\mathbb{N}_\perp \times \mathbb{N}_\perp, \mathbb{N}_\perp)$; пусть $\bar{g}$ – соответствующий ей при стандартном изоморфизме объект пространства $C(\mathbb{N}_\perp, C(\mathbb{N}_\perp, \mathbb{N}_\perp))$. Легко видеть, что $K_{\bar{g}}(\Gamma_y \supset \Gamma_x) = K_G(y|x)$, откуда и вытекает интересующее нас неравенство. Предложение 2 доказано. ▨

4.1.3. Энтропия (сложность) разрешения.

В [5] приведено следующее определении энтропии (на-

зываемой там сложностью) разрешения.

Пусть F – частично рекурсивная функция из $\mathbb{N}\times\mathbb{N}$ в $\{0,1\}$. Сложностью разрешения слова x в алфавите $\{0,I\}$ относительно F называется величина

$$KR_F(x) = \min\{\ell(p) \mid (\forall i \leq \ell(x))\ F(p,i) = x_i\}$$

Здесь $\ell(p)$ – объем натурального числа p, $\ell(x)$ – объем (=длина) слова x, x_i – i-ая буква слова x.

Среди всех частично рекурсивных функций из $\mathbb{N}\times\mathbb{N}$ в $\{0,I\}$ существует оптимальная F, для которой KR_F минимальна среди всех KR_G (с точностью до ограниченного слагаемого). Сложность разрешения слова x относительно фиксированной оптимальной функции F и называется энтропией разрешения слова x. Она обозначается $KR(x)$.

Предложение 3.

$$KR(x) \asymp K_{\mathbb{N}}(\langle \Omega, \Gamma_x \rangle)$$

(напомним, что Ω – пространство всех конечных и бесконечных последовательностей нулей и единиц, Γ_x – множество всех продолжений конечного слова x, знак $\asymp$ означает совпадение с точностью до ограниченного слагаемого).

Доказательство. Пусть F – частично рекурсивная функция, для которой KR_F минимально среди всех KR_G (с точностью до ограниченного слагаемого). Построим способ описания f объектов Ω объектами $\mathbb{N}_\perp$, положив

$$f(\perp) = \perp,\quad f(n) = F(n,0)F(n,1)\ldots F(n,k)$$

где k – наибольшее число, для которого все значения $F(n,0)$, $F(n,1),\ldots,F(n,k)$ определены. Если $F(n,i)$ определено при любом i, то положим $f(n) = F(n,0)F(n,1)\ldots$

Нетрудно видеть, что f действительно является вычислимым объектом пространства $C(\mathbb{N}_\perp,\Omega)$ и что $K_f(\langle\Omega,\Gamma_x\rangle) = KR_F(x)$.

Отсюда получаем, что при подходящем C для всех x выполне-

но неравенство $K_{\mathbb{N}_\perp}(\langle\Omega, \Gamma_x\rangle) \le KR_F(x) + C$.

Обратно, пусть f – оптимальный способ описания объектов Ω с помощью объектов $\mathbb{N}_\perp$. Рассмотрим функцию G из $\mathbb{N} \times \mathbb{N}$ в $\{0, 1\}$, определенную так:

$G(n, i)$ = i -ый член последовательности $f(n)$ (Если $f(n)$ слишком короткая и не имеет i -го члена, то $G(n, i)$ не определена для таких n и i). Функция G частично рекурсивна, так как $G(n, i) = k$ тогда и только тогда, когда существует последовательность α из $i+1$ нулей и единиц, последний член которой равен k и для которой $(n \mapsto \alpha) \le f$. Нетрудно видеть, что $KR_G(x) = K_f(\langle\Omega, \Gamma_x\rangle)$ (в самом деле, $K_f(\langle\Omega, \Gamma_x\rangle) = \inf\{\, l(t) \mid t \in \mathbb{N}_\perp, f(t)$ начинается на x $\}$ и правая часть не изменится, если исключить случай $t = \perp$, так как $\perp \le 0$ и $l(\perp) = l(0) = 0$). Отсюда следует, что при подходящем C для всех x выполнено неравенство $KR(x) \le K_f(\langle\Omega, \Gamma_x\rangle) + C$. Предложение 3 доказано. ▨

4.1.4. Префиксная энтропия.

В работе [2] дается следующее определение префиксной энтропии.

Частично рекурсивная функция из множества $\{0, 1\}$ -слов в множество натуральных чисел называется префиксной, если она удовлетворяет условию: $B(x) = B(x')$, если x – начало x', $B(x)$ и $B(x')$ определены. По префиксной функции B определяется сложность $KP_B(x) = \inf\{\, l(p) \mid B(p) = x\}$ Существует такая частично рекурсивная префиксная функция A, что для любой другой частично рекурсивной префиксной функции B найдется C, при котором для всех x справедливо

неравенство $KP_A(x) \le KP_B(x) + C$. Выберем одну из функций A, обладающих этим свойством. Соответствующую ей сложность $KP_A(x)$ будем обозначать $KP(x)$ и называть префиксной энтропией.

Следующее предложение показывает, каким образом префиксная энтропия может быть получена по нашей схеме, если пространством описаний считать Ω.

Предложение 4.

$$KP(n) \asymp K_\Omega(\langle \mathbb{N}_\perp, \Gamma_n \rangle)$$

Доказательство проходит аналогично доказательствам предложений I - 3, если воспользоваться следующей леммой.

Лемма I. (а) Пусть f - вычислимый объект пространства $C(\Omega, \mathbb{N}_\perp)$. Тогда функция F из множества конечных $\{0, I\}$-слов в $\mathbb{N}$, определяемая формулой

$$F(x) = \begin{cases} f(x), & \text{если } f(x) \ne \perp \\ \text{не определено, если } & f(x) = \perp \end{cases}$$

является префиксной и $KR_F(n) = K_f(\langle \mathbb{N}_\perp, \Gamma_n \rangle)$ для всех $n \in \mathbb{N}$.

(б) Пусть F - префиксная функция. Тогда формула

$$f(x) = \begin{cases} F(x'), \text{ если } x' \text{ - начало слова } x, \text{ на котором } F \text{ определена;} \\ \perp, \text{ если } F(x') \text{ не определено для всех начал } x' \text{ слова } x; \end{cases}$$

определяет вычислимый объект $f \in C(\Omega, \mathbb{N}_\perp)$ и $KR_F(n) = K_f(\langle \mathbb{N}, \Gamma_n \rangle)$ для всех $n \in \mathbb{N}$.

Доказательство. (а) Если $F(x)$, $F(x')$ определены и x - начало x', то $F(x) = f(x)$, $F(x') = f(x')$, $f(x) \le f(x')$ в силу монотонности f и, значит (так как $f(x) \ne \perp$), $f(x) = f(x')$. Вычислимость F и равенство $KR_F(n) = K_f(\langle \mathbb{N}, \Gamma_n \rangle)$ очевидны.

(б) Заметим прежде всего, что определение f корректно:

если x' и x'' – различные начала x, на которых F определена, то $F(x')=F(x'')$ в силу префиксности F. Непрерывность функции f легко проверяется с помощью леммы 5 из п. I.4.3.3. Вычислимость f и равенство $KR_F(n) = K_f(\langle \mathbb{N}, \Gamma_n \rangle)$ ясны. ∎

Предложение 4 доказано. ∎

4.I.5. Монотонная энтропия.

В работе [2] на с. 33 дается следующее определение монотонной энтропии.

Заданием алгоритмического оператора называется любое перечислимое множество A пар конечных последовательностей нулей и единиц, обладающее свойством:

если $\langle x,y\rangle \in A$, $\langle x',y'\rangle \in A$, x и x' совместны, то y и y' совместны (совместность = наличие общего продолжения). Пусть A – задание алгоритмического оператора, а α – конечная или бесконечная последовательность нулей и единиц. Значением A на α называется (конечная или бесконечная) последовательность нулей и единиц, полученная объединением всех таких y, что $\langle x,y\rangle \in A$ при подходящем конечном начале x последовательности α. Эта последовательность называется $A(\alpha)$.

Таким образом, каждому заданию алгоритмического оператора соответствует отображение Ω в Ω. Эти отображения и называются алгоритмическими операторами.

Для произвольного алгоритмического оператора B определяется монотонная сложность конечной последовательности x относительно B: $KM_B(x) = \inf\{l(p) \mid x \leq B(p)\}$ *)

---

*) В [2] вместо "KM" используется обозначение "km".

Существует такой алгоритмический оператор A, что для любого другого алгоритмического оператора B найдется такое C, что при всех x выполнено неравенство

$$KM_A(x) \leq KM_B(x) + C.$$

Выбираем один из операторов A, обладающих этим свойством, и соответствующую сложность $KM_A(x)$ обозначаем $KM(x)$ и называем монотонной энтропией x.

Монотонная энтропия получается по нашей схеме, если пространством описаний и пространством объектов считать пространство Ω.

Предложение 5.

$$KM(x) \asymp K_{\Omega}(\langle \Omega, \Gamma_x \rangle)$$

Доказательство. Это предложение легко следует из такой леммы.

Лемма 2. Множество алгоритмических операторов совпадает с множеством вычислимых объектов пространства $C(\Omega, \Omega)$.

Доказательство леммы. Нетрудно проверить, что каждый алгоритмический оператор задает вычислимый объект пространства $C(\Omega, \Omega)$. Обратно, пусть $f \in C(\Omega, \Omega)$ – вычислимый объект. Рассмотрим множество

$$A = \left\{ \langle x, y \rangle \;\middle|\; \begin{array}{l} x, y \text{ - конечные последовательности} \\ \text{нулей и единиц, } (x \mapsto y) \leq f \end{array} \right\}$$

Оно перечислимо. Нетрудно проверить, что оно является заданием алгоритмического оператора, совпадающего с f. ∎

Предложение 5 доказано. ∎

4.I.6. Оптимальные нумерации и энтропия.

К.П.Шнорр (см. [20], [21], [12]) ввел понятие оптимальной нумерации множества $\mathcal{T}$ частично рекурсивных функций одной переменной. Прежде чем воспроизвести определение Шнорра, на-

помним, что вычислимой нумерацией множества $\mathcal{T}$ называется всюду определенное отображение $\mathbb{N}$ на $\mathcal{T}$, образ которого есть всё $\mathcal{T}$ и функция

$$F_\nu(m,n) \simeq [\nu(m)](n)$$

есть частично рекурсивная функция из $\mathbb{N} \times \mathbb{N}$ в $\mathbb{N}$. Говорят, что всюду определенная функция h сводит нумерацию ν множества $\mathcal{T}$ к нумерации μ того же множества, если $\mu(h(n)) = \nu(n)$ для всех $n \in \mathbb{N}$.

Вычислимая нумерация μ множества $\mathcal{T}$ называется оптимальной по Шнорру, если для всякой вычислимой нумерации ν множества $\mathcal{T}$ существует общерекурсивная функция h, сводящая ν к μ, для которой при подходящем C и всех n выполнено неравенство $\ell(h(n)) \leq \ell(n) + C$

Говоря неформально, нумерация μ оптимальна, если по любому номеру любой функции в любой вычислимой нумерации ν можно указать μ -номер той же функции, причем ненамного более длинный.

Нетрудно доказать (см. [21]), что оптимальные нумерации существуют. Зафиксируем одну из таких нумераций и обозначим ее μ. Будем называть энтропией частично рекурсивной функции φ число $K(\varphi) = \inf\{\ell(n) \mid \mu(n) = \varphi\}$.

При замене μ на другую оптимальную нумерацию величина K останется неизменной с точностью до ограниченного слагаемого.

Покажем теперь, каким образом это понятие (по существу то же определение рассматривалось В.Н.Агафоновым [1]) может быть получено по нашей схеме.

<u>Предложение 6.</u>

$K(\varphi) \asymp K_{\mathbb{N}_\perp}(\langle \mathbb{F}, \{\varphi\} \rangle)$ (для частично рекурсивных φ)

Заметим, что, согласно предложению 2 из п. 2.3 и замечаниям из п. I.5.4 энтропия задачи $\langle \mathbb{F}, \{\varphi\} \rangle$ конечна для тех и только тех φ, которые являются частично рекурсивными.

<u>Доказательство</u>. Пусть $f \in C(\mathbb{N}_\perp, F)$ – оптимальный способ описания, $\mu : \mathbb{N} \to \mathcal{T}$ – оптимальная нумерация.

Рассмотрим нумерацию ν : $\nu(0) = f(\perp)$, $\nu(n+1) = f(n)$. Очевидно, ν – вычислимая нумерация множества $\mathcal{T}$. Согласно определению оптимальности, существует общерекурсивная функция h, для которой $\mu(h(n)) = \nu(n)$ и $\ell(h(n)) \leq \ell(n) + c$. Если $\nu(n) = \varphi$, то $K(\varphi) \leq \ell(h(n)) \leq \ell(n) + c$ Отсюда и из определения ν легко вывести, что $K(\varphi) \leq K_{\mathbb{N}_\perp}(\langle \mathbb{F}, \{\varphi\} \rangle) + c'$.

Докажем обратное неравенство. Пусть g – способ описания, определенный так: $g(\perp)$ = нигде не определенная функция, $g(n) = \mu(n)$. Очевидно, g является вычислимым объектом и $K_g(\langle \mathbb{F}, \{\varphi\} \rangle) \leq K(\varphi)$. ▨

4.2. Неравенства, связывающие различные виды энтропии.

В этом пункте мы покажем, каким образом многочисленные известные неравенства, связывающие различные виды энтропии, могут быть получены как следствие доказанных нами общих теорем.

Следствие I. $K(x) \preceq KP(x)$

$KM(x) \preceq KR(x)$

(Запись $f(x) \preceq g(x)$ означает, что найдется такая константа C, что для всех x верно неравенство $f(x) \le g(x) + C$.)

Доказательство. Следует воспользоваться предложениями I,3,4,5 из п. 4.I и тем, что $\mathbb{N}_\perp$ не хуже Ω (предложение 3 из п. 2.5) ▨

Следствие 2. $KP(x) \preceq K(x) + C \log_2 K(x)$

$KR(x) \preceq KM(x) + C \log_2 KM(x)$

при подходящем C.

Доказательство. Следует воспользоваться предложениями I,3,4,5 из п. 4.I и тем, что Ω почти не хуже $\mathbb{N}_\perp$ (предложение 3 из п. 2.5) ▨

В следствиях I и 2 сравнивались энтропии объектов одного сорта (чисел для K и KP и слов для KM и KR). Чтобы сравнить, к примеру, K с KR, нужно установить соответствие между натуральными числами и словами, положив, к примеру, что числу x соответствует слово, получающееся из двоичной записи числа $x+1$ отбрасыванием первой единицы. (Впрочем, годится и любое другое вычислимое взаимно однозначное соответствие.) Пользуясь этим отождествлением, мы можем говорить об энтропиях $K(x)$ и $KP(x)$ двоичного слова x.

Следствие 3. $KR(x) \preccurlyeq K(x)$

$$KM(x) \preccurlyeq KP(x)$$

Доказательство. Рассмотрим вычислимое непрерывное отображение $f: \mathbb{N}_\perp \to \Omega$, сопоставляющее объекту $\perp$ пустое слово, а каждому числу x - соответствующее в указанном смысле слово $\bar{x}$.

Так как $f(x) \subset \Gamma_{\bar{x}}$, то, согласно предложению I из п. 2.6, имеет место неравенство

$$K_X(\langle \Omega, \Gamma_{\bar{x}} \rangle) \preccurlyeq K_X(\langle \mathbb{N}_\perp, \{x\} \rangle)$$

Остается взять Ω и $\mathbb{N}_\perp$ в качестве X и сослаться на предложения I,3,4,5 из п. 4.I. ▨

Учитывая очевидное неравенство $K(x) \preccurlyeq \ell(x)$ и следствия I - 3, получаем такое

Следствие 4. $K(x) \preccurlyeq \ell(x)$

$$KP(x) \preccurlyeq \ell(x) + C \log_2 \ell(x) \text{ ▨}$$

Чуть более сложно доказывается

Следствие 5. $K(x) \preccurlyeq KR(x) + C \log_2 \ell(x)$

при подходящем C.

Доказательство. Рассмотрим вычислимую непрерывную функцию f из $\Omega \times \mathbb{N}_\perp$ в $\mathbb{N}_\perp$. Именно, положим

$$f(y,k) = \begin{cases} \text{число, соответствующее начальному отрезку слова } y \text{ длины } k \text{, если} \\ k \in \mathbb{N} \text{ и } \ell(y) \geq k \\ \perp \text{, если } k = \perp \text{ или } \ell(y) < k \end{cases}$$

Применяя к ней предложение I из п. 2.6, получаем, что

$$K_{\mathbb{N}_\perp}(\langle \mathbb{N}_\perp, \{x\} \rangle) \leq K_{\mathbb{N}_\perp}(\langle \Omega, \Gamma_{\bar{x}} \rangle \wedge \langle \mathbb{N}_\perp, \ell(\bar{x}) \rangle)$$

Применяя следствие 2 предложения I из п. 2.2, это неравенство можно продолжить так:

$$K(x) = K_{\mathbb{N}_\perp}(\langle \mathbb{N}, \{x\}\rangle) \leq K_{\mathbb{N}_\perp}(\langle \Omega, \Gamma_{\bar{x}}\rangle) + K(l(\bar{x})) +$$
$$+ c_1 \log_2 (K_{\mathbb{N}_\perp}(\langle \Omega, \Gamma_{\bar{x}}\rangle) + K(l(\bar{x}))) \leq KR(x) + C \log l(x)$$

(при последнем переходе мы пользуемся неравенствами из следствия 4).

Объединяя доказанные результаты, можно составить таблицу

описания / объекты	$\mathbb{N}_\perp$	Ω
$\mathbb{N}_\perp$	K $\leq$	KP
	$\vee\!/$	$\vee\!/$
$\Omega_\perp$	KR	KM

В этой таблице KR - наименьшая, KP - наибольшая из энтропий; из следствий 4 и 5 вытекает, что они (и, значит, все четыре энтропии) отличаются не более чем на $C \log_2 l(x)$

Покажем, что эта оценка точная, то есть что разница между любыми двумя энтропиями из этой таблицы может быть по порядку равна $\log l(x)$. Достаточно рассмотреть две "средних" энтропии K и KM и показать, что разница между ними принимает как положительные, так и отрицательные значения, по порядку равные $\log l(x)$.

<u>Предложение I</u>. Существует константа C и бесконечно много таких x , что $K(x) - KM(x) \geq \log_2 l(x) - C$ а также бесконечно много таких x , что $KM(x) - K(x) \geq$ $\geq \log_2 l(x) - C$

<u>Доказательство</u>. I. Пусть слово x_n состоит из n нулей. Тогда $K(x_n) \asymp K(n)$ (напомним, что через $K(n)$ обозначается простая колмогоровская энтропия числа n , через $K(x_n)$- энтропия числа, соответствующего слову x_n), в то время как $KM(x_n) \asymp 0$. Поэтому для тех n , для которых выполняет-

ся неравенство $K(n) \geq \log_2 n - 1$, выполняется и неравенство $K(x_n) - KM(x_n) \geq \log_2 l(x_n) - C$. Таких n бесконечно много (см. [5]), поэтому и слов x, для которых $K(x) - KM(x) \geq \log_2 l(x) - C$, бесконечно много.

2. Рассмотрим последовательность слов x_n, ни одно из которых не является началом другого, для которой

$$l(x_n) \leq \log_2 n + 2\log_2 \log_2 n + C$$

построенную при доказательстве предложения 3 из п. 2.5. Имеем: $K(x_n) \asymp K(n) \leq \log_2 n + C$. С другой стороны, прообразы множеств Γ_{x_n} при оптимальном способе описания $f \in C(\Omega, \Omega)$ не пересекаются, поэтому

$$\sum_{n=1}^{N} \frac{1}{2^{KM(x_n)}} \leq 1$$

Сравнивая это неравенство с неравенством

$$\sum_{n=1}^{N} \frac{1}{2^{K(x_n)}} \geq C_1 \sum_{n=1}^{N} \frac{1}{n} \geq C_2 \log_2 N$$

мы видим, что для любого N найдется такое $n \leq N$, что n-ый член второй суммы в $C_2 \log_2 N$ раз больше n-го члена первой, то есть

$$\frac{1}{2^{K(x_n)}} \geq C_2 \log_2 N \cdot \frac{1}{2^{KM(x_n)}}$$

или $\quad K(x_n) \leq KM(x_n) - \log_2 \log_2 N + C_3 \qquad (*)$

и $KM(x_n) - K(x_n) \geq \log_2 \log_2 N - C_3$

Остается заметить, что $\log_2 \log_2 N \geq \log_2 \log_2 n \geq \log_2 l(x_n) - C_4$ (см. выше неравенство для длины x_n) и что среди слов x_n, построенных указанным способом для разных N, бесконечно много различных (это вытекает из неравенства (*)).

4.3. Априорная вероятность и ее свойства.

В работе [2] вводится понятие априорной вероятности. В этом пункте мы проанализируем свойства этого понятия с точки зрения нашей общей схемы.

Пусть X – произвольное пространство, $f \in C(\Omega, X)$ – способ описания. С каждой задачей $\alpha = \langle X, A \rangle$, для которой A является борелевским подмножеством пространства X, свяжем число

$$P_f(\alpha) = \mu(\{\omega \in \Omega \setminus \Omega^* \mid f(\omega) \in A\})$$

где μ – равномерная бернуллиевская мера на множестве $\Omega \setminus \Omega^*$ бесконечных последовательностей нулей и единиц (через Ω^* мы обозначаем множество конечных последовательностей нулей и единиц). Это число представляет собой вероятность такого события: при бросании симметричной монеты возникнет последовательность нулей и единиц (соответствующих орлам и решкам), являющаяся описанием решения задачи α. Коротко мы будем называть число $P_f(\alpha)$ вероятностью решения задачи α при способе описания f.

Предложение I. Среди всех способов описания существует оптимальный, то есть такой способ описания $f \in C(\Omega, X)$ что для любого другого способа $g \in C(\Omega, X)$ найдется такое $c > 0$, что для любой задачи α в пространстве X выполнено неравенство $P_f(\alpha) \geqslant c \cdot P_g(\alpha)$.

Доказательство. Пусть $h : \Omega \to \Omega \times \mathbb{N}_\perp$ – способ описания, при котором $h(0^n 1 x) = \langle x, n \rangle$ при всех $n \in \mathbb{N}$ и $x \in \Omega$, а $h(0^k) = \perp$ (здесь 0^s обозначает слово из s нулей). Для этого способа описания выполнено такое неравенство: если $B \subset \Omega \setminus \Omega^*$ – борелевское множе-

ство, то $\mu(h^{-1}(B\times\{n\}))=\frac{1}{2^{n+1}}\mu(B)$

В самом деле, $h^{-1}(B\times\{n\})$ состоит из всех последовательностей вида 0^n1x, где $x\in B$. Рассмотрим теперь вычислимый объект $u\in C(\Omega\times\mathbb{N}_\perp,X)$, среди сечений $u_n: x\mapsto u(\langle x,n\rangle)$ которого встречаются все вычислимые объекты пространства $C(\Omega,X)$ (см. п. I.5.5, следствие предложения I). В качестве искомого оптимального способа описания возьмем композицию h и u: $f=u\circ h\in C(\Omega,X)$. Если g – любой способ описания из $C(\Omega,X)$, то существует $n\in\mathbb{N}$, для которого $g(x)=u(\langle x,n\rangle)$ при всех x. Пусть A – произвольное борелевское подмножество X. Пусть $B=\{\omega\in\Omega\setminus\Omega^* \mid g(\omega)\in A\}$. Очевидно, $u(B\times\{n\})\subset A$ и $h^{-1}(B\times\{n\})\subset\{\omega\in\Omega\setminus\Omega^*\mid u(h(\omega))\in A\}=$ $=\{\omega\in\Omega\setminus\Omega^*\mid f(\omega)\in A\}$, поэтому $P_f(\langle X,A\rangle)=$
$=\mu(\{\omega\in\Omega^*-\Omega\mid f(\omega)\in A\})\geq\mu(h^{-1}(B\times\{n\}))=$
$=\frac{1}{2^{n+1}}\mu(B)=\frac{1}{2^{n+1}}P_g(\langle X,A\rangle)$

Таким образом, в качестве C можно взять $\frac{1}{2^{n+1}}$.

Предложение I доказано. ▨

Выбрав и зафиксировав некоторый оптимальный способ f, мы будем называть $P_f(\alpha)$ априорной вероятностью задачи α и обозначать $P(\alpha)$.

Пусть $X=\mathbb{N}_\perp$. Априорную вероятность задачи $\langle\mathbb{N}_\perp,\Gamma_n\rangle$ будем называть априорной вероятностью числа n. Аналогичным образом при $X=\Omega$ мы будем называть априорную вероятность задачи $\langle\Omega,\Gamma_x\rangle$ априорной вероятностью слова x.

Предложение 2. Введенные таким образом априорные вероятности чисел и слов совпадают (с точностью до ограниченного множителя) с введенными в [2] на с. 26 (априорное распределение вероятностей на $\mathbb{N}$) и с. 40 (полумера M из теор.

4.I; см. также [5], с. I07)

Доказательство этого предложения мы отложим; предварительно нам нужно изучить некоторые свойства введенных понятий.

Пусть X – некоторое пространство. Меру[ж)] P, определенную на семействе борелевских подмножеств X, мы будем называть перечислимой, если множество $\{\langle n,r\rangle \in \mathbb{N}\times\mathbb{Q} \mid r < P(\Gamma_{\nu(n)})\}$ перечислимо (здесь ν – нумерация всех конечных объектов пространства X, фигурирующая в определении эффективного f_0-пространства).

<u>Предложение 3</u>. Априорная вероятность является перечислимой мерой.

<u>Доказательство</u>. В самом деле,

$$P(\Gamma_x) = \mu(\{\omega \in \Omega \setminus \Omega^* \mid x \leq f(\omega)\} =$$
$$= \mu(\cup\{I_t \mid t \in \Omega^*,\ (x \mapsto t) \leq f\})$$

где I_t – множество всех бесконечных последовательностей нулей и единиц, начинающихся на t. Так как множество тех n и t, для которых $(\nu(n) \mapsto t) \leq f$, перечислимо (ибо f вычислим), из написанного равенства вытекает перечислимость априорной вероятности.

Предложение 4. Если множество конечных объектов пространства X является деревом[жж)], то априорная вероятность на является максимальной (с точностью до ограниченного и отде-

---

ж) Мы рассматриваем только меры с конечными значениями, не оговаривая этого специально.

жж) Деревом мы называем частично упорядоченное множество, обладающее таким свойством: из $x \leq z$ и $y \leq z$ следует, что $x \leq y$ или $y \leq x$.

ленного от нуля множителя) среди всех перечислимых мер: для всякой перечислимой меры R существует константа $C>0$, такая, что для любого борелевского $A\subset X$ выполнено неравенство $P(\langle X,A\rangle)\geqslant C\cdot R(A)$

Из этого утверждения вытекает утверждение предложения 2, так как априорная вероятность (на $\mathbb{N}$ и Ω) определялась в [2] как максимальная перечислимая мера на этих пространствах, а в них множество конечных объектов является деревом и, следовательно, к ним применимо утверждение предложения 4.

<u>Доказательство предложения 4</u>. Утверждение предложения 4 следует из определения априорной вероятности и такой леммы.

<u>Лемма I</u>. Пусть множество конечных объектов пространства X является деревом. Пусть R – перечислимая мера на X и $R(X)\leqslant 1$. Тогда существует способ описания $h\in C(\Omega,X)$, для которого $R(A)=P_h(\langle X,A\rangle)$.

Если эту лемму считать доказанной, то, поделив любую заданную перечислимую меру S на достаточно большое целое число N, имеем $\frac{S}{N}(X)\leqslant 1$, поэтому $\frac{S}{N}$ представимо в виде P_h и не превосходит $C'\cdot P$ в силу определения априорной вероятности. Поэтому предложение 4 вытекает из леммы I. Осталось доказать лемму I. Предварительно нам понадобится ряд определений и лемм технического характера.

Пусть на конечном множестве $A\subset\mathbb{N}$ задан частичный порядок, превращающий его в дерево (т.е. из $x\leq z$ и $y\leq z$ следует $x\leq y$ или $y\leq x$). Пусть каждому $x\in A$ сопоставлено двоично-рациональное число $r(x)$ (двоично-рациональное число = рациональная дробь, знаменатель которой есть степень 2), причем выполнены такие свойства:

(а) если $x \le y_1, \ldots, x \le y_n$, $y_1, \ldots, y_n$ попарно не сравнимы, то $\tau(x) \ge \tau(y_1) + \ldots + \tau(y_n)$

(б) если $y_1, \ldots, y_n$ попарно не сравнимы, то

$$\tau(y_1) + \ldots + \tau(y_n) \le 1.$$

В этом случае мы будем называть тройку $\langle A$, порядок на A, $\tau \rangle$ схемой.

Пример схемы:

В данном пункте мы будем называть конечные последовательности нулей и единиц коротко словами (вместо более полного "слова в алфавите $\{0,1\}$). Конечное множество слов, в котором ни одно слово не является началом другого, мы будем называть набором. Будем говорить, что набор N_2 шире набора N_1, если всякое слово из N_1 является продолжением некоторого слова из N_2. С каждым набором N мы свяжем множество $[N]$ всех бесконечных продолжений всех слов набора N. Очевидно, что если N_2 шире N_1, то $[N_2] \supset [N_1]$. (Обратное, вообще говоря, не верно.) Меру множества $[N]$ мы будем называть мерой набора N и обозначать $|N|$. Очевидно,

$$|N| = \sum \{ 2^{-\ell(x)} \mid x \in N \}$$

Пусть дана схема $S = \langle A, \le, \tau \rangle$. Функцию φ, сопоставляющую каждому $x \in A$ набор $\varphi(x)$, мы назовем реализацией схемы S, если выполнены такие свойства:

(а) если $a, b \in A$, $a \le b$ в смысле порядка на A, то $\varphi(a)$ шире $\varphi(b)$.

(б) если $a, b \in A$, a и b не сравнимы, то

$$[\varphi(a)] \cap [\varphi(b)] = \emptyset$$

(в) для всех $a \in A$ имеет место равенство $r(a) = |\varphi(a)|$

Лемма 2. Всякая схема имеет реализацию. Реализацию можно эффективно найти по схеме.

Доказательство. Отметим следующее очевидное свойство наборов: если $\mathcal{N}$, $\mathcal{N}_1, \ldots, \mathcal{N}_k$ – наборы, $\mathcal{N}$ шире всех $\mathcal{N}_i$, $[\mathcal{N}_i] \cap [\mathcal{N}_j] = \emptyset$, r – двоично-рациональное число, причем $r \leq |\mathcal{N}| - |\mathcal{N}_1| - \ldots - |\mathcal{N}_k|$, то существует набор $\mathcal{N}_{k+1}$ для которого $[\mathcal{N}_i] \cap [\mathcal{N}_{k+1}] = \emptyset$ при всех i, $\mathcal{N}$ шире $\mathcal{N}_{k+1}$, $|\mathcal{N}_{k+1}| = r$.

Пусть $\langle A, \leq, r \rangle$ – схема. Каждому $x \in A$ сопоставим натуральное число, называемое уровнем x и обозначаемое $u(x)$. Именно, минимальные элементы множества A объявим элементами уровня 0, а уровнем любого не минимального элемента будем считать число, на единицу большее уровня его непосредственного предшественника (наибольшего среди всех меньших его элементов; таковой существует в силу определения схемы). Пусть $x_1, \ldots, x_p$ – все элементы уровня 0. Нам надо построить наборы $\mathcal{N}_1, \ldots, \mathcal{N}_p$, для которых $|\mathcal{N}_i| = r(x_i)$ и $[\mathcal{N}_i] \cap [\mathcal{N}_j] = \emptyset$. Мы построим их по очереди, пользуясь отмеченным выше свойством наборов (в нем в качестве $\mathcal{N}$ надо взять набор, единственным элементом которого является пустое слово, в качестве $N_1, \ldots, N_k$ – уже построенные наборы, N_{k+1} – очередной строимый набор; неравенство $r \leq |\mathcal{N}| - |N_1| - \ldots - |N_k|$ т.е. $r(x_{k+1}) \leq 1 - r(x_1) - \ldots - r(x_k)$, выполнено, так как $r(x_1) + \ldots + r(x_{k+1}) \leq 1$ по определению схемы.

После того как построены все наборы, соответствующие элементам уровня 0, мы переходим к элементам уровня I. Все элементы уровня I разбиваются на p групп – к i-ой группе относятся те элементы уровня I, непосредственным предшественни-

ком которых является x_p . Для каждой группы построение соответствующих наборов будем проводить независимо. Построение проводится аналогично уже рассмотреному; в качестве N берется один из наборов $N_1, \ldots, N_p$ и используется неравенство

$$|N_i| \geq \sum \left\{ \tau(t) \,\middle|\, \begin{array}{l} t \text{ - элемент уровня 1, непосредственным предшественником которого является элемент } x_i \end{array} \right\}$$

следующее из определения схемы (любые две вершины одного уровня несравнимы). Затем строятся наборы, соответствующие элементам уровня 2 и т.д. Таким образом мы завершим построение реализации данной схемы. Ясно, что описанное построение эффективно - существует алгоритм, дающий по схеме (точнее, по ее номеру в естественной нумерации) ее реализацию. Лемма 2 доказана. ▨

Пусть $S_1 = \langle A_1, \leq_1, \tau_1 \rangle$ и $S_2 = \langle A_2, \leq_2, \tau_2 \rangle$ - две схемы. Будем говорить, что схема S_2 является *расширением* схемы S_1 , если выполнены следующие условия:

(а) $A_1 \subset A_2$;

(б) порядок, индуцированный из $\leq_2$ на A_1, совпадает с $\leq_1$;

(в) если $a \in A_1$, то $\tau_2(A) \geq \tau_1(A)$

Будем говорить также, что реализация φ_2 схемы S_2 является расширением реализации φ_1 схемы S_1 , если S_2 есть расширение S_1 и при всех $x \in A_1$ набор $\varphi_2(x)$ шире набора $\varphi_1(x)$.

Лемма 3. Пусть φ_1 - реализация схемы S_1 , а схема S_2 является расширением схемы S_1 . Тогда можно построить реализацию φ_2 схемы S_2 , являющуюся расширением φ_1. Это построение можно выполнить эффективно.

Доказательство. В частично упорядоченном множестве наборов ($\mathcal{N}_1 \leq \mathcal{N}_2 \rightleftarrows \mathcal{N}_2$ шире $\mathcal{N}_1$) любые два набора $\mathcal{N}_1$ и $\mathcal{N}_2$ имеют точную верхнюю грань:

$$x \in sup(N_1, N_2) \Leftrightarrow \left(\begin{array}{l} x \in N_1 \cup N_2 \text{ и никакое собственное начало} \\ \text{слова } x \text{ не принадлежит } N_1 \cup N_2 \end{array} \right)$$

Ее мы будем называть объединением наборов N_1 и N_2. Пусть $S_1 = \langle A_1, \leq_1, \tau_1 \rangle$ и $S_2 = \langle A_2, \leq_2, \tau_2 \rangle$ – две схемы, S_2 – расширение S_1, φ_1 – реализация схемы S_1. Построим схему S_1' и ее реализацию φ_1' следующим образом:

$S_1' = \langle A_2, \leq_2, \tau_1' \rangle$, где

$$\tau_1'(x) = sup \left\{ \sum_{y \in T} \tau_1(y) \;\middle|\; \begin{array}{l} T \subset A_1 \text{, элементы } T \text{ попарно несрав-} \\ \text{нимы и } x \leq_2 t \text{ для всех } t \in T \end{array} \right\}$$

$\varphi_1'(x)$ = объединение $\{\varphi_1(y) \mid y \in A_1, x \leq_2 y\}$

Очевидно, $[\varphi_1'(x)] = \cup \{[\varphi_1(y)] \mid y \in A_1, x \leq_2 y\}$

Проверим, что $|\varphi_1'(x)| = \tau_1'(x)$. В самом деле, если $T \subset A_1$, элементы T попарно несравнимы и больше или равны x, то множества $[\varphi_1(y)]$ при $y \in T$ попарно не пересекаются, $[\varphi_1'(x)] \supset \cup \{[\varphi_1(y)] \mid y \in T\}$, $|\varphi_1'(x)| = \mu[\varphi_1'(x)] \geq$ $\geq \sum \{\mu(\varphi_1(y)) \mid y \in T\} = \sum \{\tau_1(y) \mid y \in T\}$

Поэтому $|\varphi_1'(x)| \geq \tau_1'(x)$. Чтобы доказать обратное неравенство, выберем в качестве T множество всех тех элементов $y \in A_1$, для которых $y \geq x$ и не существует $z < y$, для которого было бы $z \geq x$ и $z \in A_1$. Тогда $[\varphi_1'(x)] = \cup \{[\varphi_1(y)] \mid y \in T\}$, $[\varphi_1(y)] \cap [\varphi_1(y')] = \emptyset$ при $y, y' \in T$, $y \neq y'$, поэтому $|\varphi_1'(x)| = \sum_{y \in T} |\varphi_1(y)| \leq \tau_1'(x)$.

Ясно также, что при $x \leq x'$ набор $\varphi_1(x)$ шире набора $\varphi_1'(x')$ и. что при несравнимых x и x' множества $[\varphi_1'(x)]$ и $[\varphi_1'(x')]$ не пересекаются – они есть объединения двух семейств множеств, причем члены первого семейства не пересекаются с членами второго (иначе x и x' имели бы общую верхнюю грань и были бы сравнимы). Отсюда легко вывести, что S_1' является схемой,

φ_1' - её реализацией, S_1' расширяет S_1, а φ_1' - φ_1. Ясно, что S_2 является расширением S_1', так как $\sum_{y\in T} r_1(y)$ (если $T\subset A_1$, элементы T попарно несравнимы и $x\leq t$ для всех $t\in T$) не превосходит $\sum_{y\in T} r_2(y)$, что не превосходит $r_2(x)$ так как S_2 является схемой.

Таким образом, заменив S_1 и φ_1 на S_1' и φ_1', можно при доказательстве леммы 3 ограничиться случаем $A_1 = A_2$.

Итак, пусть на одном и том же упорядоченном множестве A заданы две функции r_1 и r_2, превращающие его в схемы S_1 и S_2, причем $r_1\leq r_2$. Пусть φ_1 - реализация схемы S_1. Построим реализацию φ_2 схемы S_2, являющуюся расширением реализации φ_1. Построение будет производиться, как и при доказательстве леммы 2, по уровням. Пусть для элементов A уровней I,2,...,i значения φ_2 уже построены. Пусть $y_1,\ldots,y_s$ - все те элементы $i+1$-го уровня, непосредственным предшественником которых является элемент x из i-го уровня. Мы имеем наборы $\varphi_1(x)$, $\varphi_1(y_1)$, ..., $\varphi_1(y_s)$ и $\varphi_2(x)$. Построим набор $\varphi_2(y_1)$. Для этого обозначим через r число $r_2(y_1)-r_1(y_1)$. Так как $r+|\varphi_1(y_1)|+\ldots+|\varphi_1(y_s)|\leq r+r_1(y_1)+\ldots+r_1(y_s)\leq r_2(y_1)+\ldots+r_2(y_s)\leq r_2(x)$ и $\varphi_2(x)$ шире $\varphi_1(x)$, который шире всех $\varphi_1(y_i)$, то можно найти такой набор N, что $|N|=r$, $[N]$ не пересекается с $[\varphi_1(y_1)],\ldots,[\varphi_1(y_s)]$, $\varphi_2(x)$ шире N. Теперь положим $\varphi_2(y_1)$ равным объединению наборов N и $\varphi_1(y_1)$. После этого найдем набор N', для которого $\varphi(x_2)$ шире N', $|N'|=r_2(y_2)-r_1(y_2)$, $[N']$ не пересекается с $[\varphi_2(y_1)]$, $[\varphi_1(y_2)]$, $[\varphi_1(y_3)],\ldots,[\varphi_1(y_s)]$ и положим $\varphi_2(y_2)$ равным объединению $\varphi_1(y_2)$ и N'. Аналогичным образом мы определим

$\varphi_2(y_i)$ для всех $i=1,2,\ldots,s$. Так мы продолжим построение реализации φ_2 еще на один уровень.

Легко проверить, что описанное построение действительно приводит к реализации, являющейся расширением исходной. Лемма 3 доказана. ▨

Теперь мы можем дать

Доказательство леммы I. По условию, множество $\{\langle r,n\rangle \mid r\in\mathbb{Q},\ n\in\mathbb{N},\ r<R(\Gamma_{\nu(n)})\}$ перечислимо (ν - нумерация множества конечных объектов, входящая в определение эффективного f_0-пространства). Будем представлять себе для наглядности процесс перечисления этого множества развертывающимся во времени; кроме того, будем учитывать лишь те появляющиеся в ходе перечисления пары $\langle r,n\rangle$, где r - двоично-рациональное число, $r>0$.

Пусть к некоторому моменту времени обнаружилось, что выполняются неравенства $r_1<R(\Gamma_{x_1}),\ldots,r_s<R(\Gamma_{x_s})$ где $x_1,\ldots,x_s$ - некоторые конечные объекты пространства X, заданные своими номерами (т.е. соответствующие пары появились в ходе перечисления). С течением времени (т.е. в ходе перечисления) оценки снизу для $R(\Gamma_{x_i})$ увеличиваются; кроме того, появляются оценки для $R(\Gamma_{x_i})$ при новых, ранее не встречавшихся, x_i. В каждый момент времени рассмотрим схему, построенную следующим образом. Пусть $x_1,\ldots,x_i$ - появившиеся к этому моменту времени объекты (в порядке их появления). Схема будет состоять из множества $A=\{1,2,\ldots,i\}$ с порядком, заданным формулой $i\le j \Leftrightarrow x_i\le x_j$ (неравенство в правой части понимается в соответствии со структурой пространства в X); функция r задается формулой

$$\tau(a) = \sup\left\{ \sum_{k\in T} \tau_k \;\middle|\; \begin{array}{l} T\subset\{1,\dots,i\},\ a\le t \text{ для всех } t\in T \\ \text{(в смысле порядка на A), элементы } T \text{ по-} \\ \text{парно несравнимы в смысле того же порядка} \end{array} \right\}$$

Докажем, что действительно получается схема. Пусть $x, y_1, \dots$ $\dots y_n \in A$, $x \le y_1, \dots, y_n$, и $y_1, \dots, y_n$ попарно не сравнимы. Докажем, что $\tau(x) \ge \tau(y_1) + \dots + \tau(y_n)$. По определению существуют множества $T_1, \dots, T_n$, для которых $\tau(y_i) = \sum_{k\in T_i} \tau_k$, $y_i \le T_i$, элементы T_i не сравнимы. Элементы различных T_i также не сравнимы; если $t_i \in T_i$, $t_j \in T_j$, $t_i \le t_j$ то $y_i \le t_i \le t_j$ и $y_j \le t_j$, что противоречит несравнимости y_i и y_j. Таким образом, взяв в качестве T объединение всех T_i, мы видим, что $\tau(x) \ge \sum_{k\in T} \tau_k = \tau(y_1) + \dots + \tau(y_n)$

Докажем теперь, что $\tau(a) < R(\Gamma_{x_a})$. В самом деле,

$$\tau(a) = \sum_{k\in T} \tau_k < \sum_{k\in T} R(\Gamma_{x_k}) \le R(\Gamma_{x_a})$$

так как все Γ_{x_k} суть части Γ_{x_a} (ибо $x_a \le x_k$) и не пересекаются (так как x_k попарно не сравнимы). Из доказанного неравенства вытекает, что если $y_1, \dots, y_n$ попарно не сравнимы, то $\tau(y_1) + \dots + \tau(y_n) \le 1$, т.к. каждое слагаемое не превосходит меры соответствующего множества, а эти множества не пересекаются.

Итак, в каждый момент времени (=на каждом шагу перечисления) мы имеем некоторую схему. Обозначим возникающие схемы $S_1, S_2, \dots; S_i = \langle A_i, \le_i, \tau_i \rangle$. Очевидно, S_{i+1} является расширением S_i. С помощью лемм 2 и 3 построим вычислимую последовательность $\varphi_1, \varphi_2, \dots$ реализаций схем $S_1, S_2, \dots$ в которой φ_{i+1} является расширением φ_i.

С каждой реализацией φ_i свяжем объект $h_i \in C(\Omega, X)$ Именно, положим

$h_i(u)$ = наибольшее из тех x_p, для которых u является продолжением одного из слов набора $\varphi_i(x_p)$

Наибольшее из таких x_p существует, так как если u является продолжением одного из слов набора $\varphi_i(p)$ и одного из слов набора $\varphi_i(q)$, то $[\varphi_i(p)]\cap[\varphi_i(q)]\neq\emptyset$ и, по определению реализации, p и q сравнимы и, значит, $x_p \le x_q$ или $x_q \le x_p$.

Заметим, что множество $\{\omega \mid h_i(\omega)\in\Gamma_{x_q}\}$ совпадает с множеством $[\varphi_i(q)]$ (если $h_i(\omega)\geqslant x_q$, то $\omega\in[\varphi_i(p)]$ при некотором p, для которого $x_p\geqslant x_q$, поэтому $[\varphi_i(p)]\subset$ $\subset[\varphi_i(q)]$ и $\omega\in[\varphi_i(q)]$; обратное утверждение очевидно) и поэтому мера этого множества равна $r_i(q)$.

Очевидно, последовательность h_i является вычислимой возрастающей последовательностью конечных объектов $C(\Omega,X)$ Рассмотрим ее точную верхнюю грань. Это - вычислимый объект пространства $C(\Omega,X)$; обозначим его h.
Очевидно, $\{\omega \mid h(\omega)\in\Gamma_{x_q}\} = \bigcup\limits_i\{\omega \mid h_i(\omega)\in\Gamma_{x_q}\}$
Справа стоит объединение возрастающей последовательности множеств, поэтому его мера равна точной верхней грани мер множеств возрастающей последовательности, т.е. точной верхней грани множества $\{r_i(q) \mid i\in\mathbb{N}\}$. Мы знаем, что все $r_i(q)$ меньше $R(\Gamma_{x_q})$, поэтому и их точная верхняя грань не превосходит $R(\Gamma_{x_q})$. С другой стороны, $r_i(q)$ не меньше имеющейся (в момент времени i) нижней оценки для $R(\Gamma_{x_q})$. Поэтому точная верхняя грань равна $R(\Gamma_{x_q})$. Итак,
$\mu(\{\omega \mid h(\omega)\in\Gamma_{x_q}\})=R(\Gamma_{x_q})$, и, следовательно, для любого борелевского множества A выполнено равенство
$\mu(\{\omega \mid h(\omega)\in A\})=R(A)$, т.е. $P_h=R$. Лемма I доказана. ▨
Вместе с ней доказано и предложение 4. ▨

Покажем теперь, что в предложении 4 условие, требующее, чтобы множество конечных объектов пространства X было

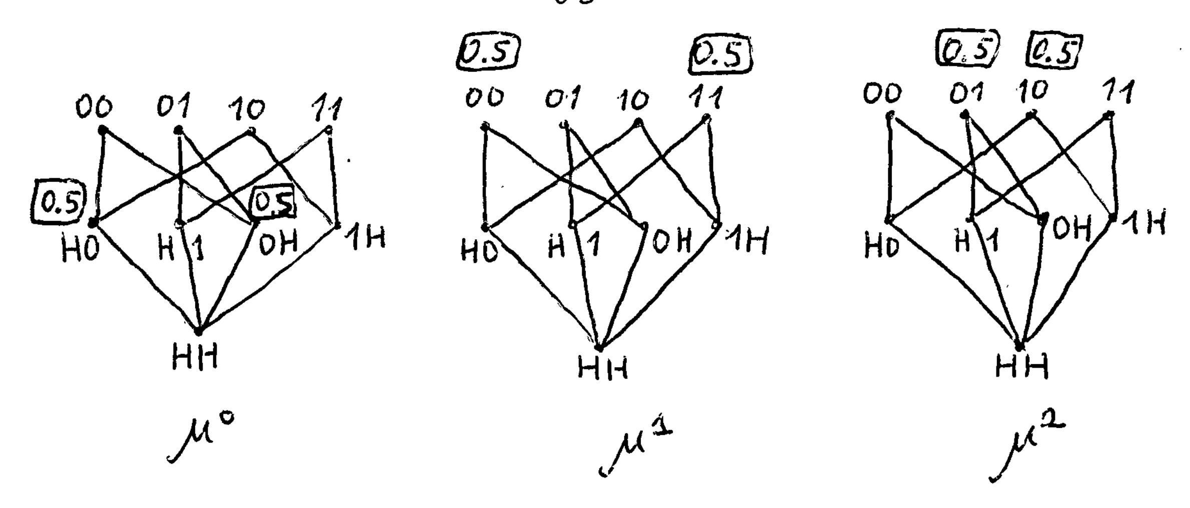
деревом, существенно. Именно, докажем такое

Предложение 5. В пространстве Ξ априорная вероятность не является максимальной перечислимой мерой: существует такая перечислимая мера R, что для любой константы $C>0$ найдется такое множество A, что $P(\langle \Xi, A\rangle) < \frac{R(A)}{C}$.

Доказательство. Напомним (см. п. I.2), что через Ξ мы обозначаем пространство частичных функций из $\mathbb{N}$ в 0,I Установим взаимно-однозначное соответствие между Ξ и пространством бесконечных последовательностей, составленных из символов 0,I,H (H – первая буква слова "неопределенность"). Именно, элементу $u \in \Xi$ соответствует последовательность, i-ый член которой равен 0, если $u(i)=0$, равен I, если $u(i)=1$, и равен H, если $u(i)$ не определено. В пространстве {0,I,H}-последовательностей рассмотрим естественную топологию (произведение счетного числа трехэлементных пространств с дискретными топологиями). Установленое соответствие не будет гомеоморфизмом, но будет переводить борелевские множества в борелевские. Поэтому, вводя искомую меру, мы будем рассматривать ее как меру на пространстве {0,I,H}-последовательностей. Последнее мы будем рассматривать как произведение счетного числа девятиэлементных пространств

$$\mathcal{U}_i = \{00, 01, 10, 11, 0H, 1H, H0, H1, HH\},$$

отождествляя {0, I, H}-последовательность с последовательностью пар символов, получаемой из исходной группировкой в пары. Итак, мы отождествляем Ξ с $\mathcal{U}_0 \times \mathcal{U}_1 \times \ldots$. Рассматриваемая мера R будет произведением счетного числа мер μ_i на $\mathcal{U}_i$ Каждая мера μ_i будет совпадать с одной из трех следующих мер (на рисунке те элементы, около которых написано число, имеют такую меру, остальные имеют меру 0):

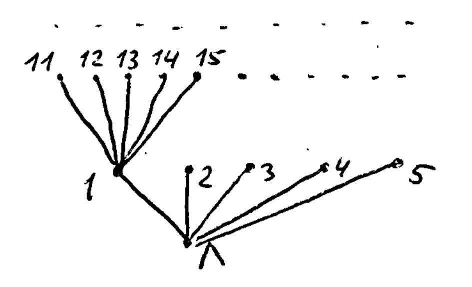


Множества P_1 и P_2 тех i, для которых $\mu_i = \mu^1$ и $\mu_i = \mu^2$, окажутся перечислимыми. Это гарантирует перечислимость возникающей на пространстве Ξ меры. В самом деле, рассмотрим вместе с мерой R меры R_k, получающиеся, если перечислимые множества P_1 и P_2 заменить на их конечные подмножества, состоящие из элементов, появившихся при перечислении до момента k. Для любого конечного элемента $x \in \Xi$ имеем $R_k(\Gamma_x) \leq R_{k+1}(\Gamma_x)$, так как для любого t в частично упорядоченном множестве U_i (естественный порядок которого указан на рисунке: элемент больше, если он нарисован выше и соединен линией) $\mu^0(\Gamma_t) \leq \mu^1(\Gamma_t)$ и $\mu^0(\Gamma_t) \leq \mu^2(\Gamma_t)$. Очевидно также, что $\lim_{k\to\infty} R_k(\Gamma_x) = R(\Gamma_x)$, так как мера множества Γ_x зависит от мер лишь на конечном числе сомножителей и при достаточно большом k имеет место равенство $R_k(\Gamma_x) = R(\Gamma_x)$. Поскольку $R_k(\Gamma_x)$ можно эффективно вычислить по k и x, мы получаем, что R действительно является перечислимой мерой.

Покажем теперь, каким образом следует выбирать меры μ_i на множествах U_i, с произведением которых мы отождествили пространство Ξ. Процесс выбора этих мер мы будем представ-

лять себе для наглядности развивающимся во времени. В начальный момент времени во всех сомножителях выбирается мера μ^0. Затем в некоторых из них она может быть заменена на меру μ^1 или на меру μ^2. Появившиеся в некоторый момента меры μ^1 и μ^2 более не меняются. Поскольку процесс эффективен, это гарантирует перечислимость рассмотренных выше множеств P_1 и P_2.

Для описания выбора мер нам понадобятся некоторые приготовления. Рассмотрим дерево всех слов в алфавите $\{1,2,3,4,5\}$.



Выберем и зафиксируем некоторый вычислимый способ, сопоставляющий каждой его вершине p некоторое натуральное число $N(p)$, причем разным вершинам – разные. В дальнейшем мы будем связывать с вершиной p сомножитель $U_{N(p)}$ в произведении $U_0 \times U_1 \times \ldots$ Сопоставим теперь каждой вершине p конечный объект $\varkappa(p)$ пространства $\widehat{\Xi}$. Именно, $\varkappa(\Lambda)=\bot$; если t – один из символов 1,2,3,4,5, то $\varkappa(pt)$ получается из $\varkappa(p)$ доопределением в точках $a = 2N(p)$ и $b = 2N(p)+1$ (т.е. в точках, соответствующих сомножителю $U_{N(p)}$ при отождествлении $\widehat{\Xi}$ с $U_0 \times U_1 \times \ldots$):

(НО) если $t=1$, то $\varkappa(pt) = \sup(\varkappa(p), (b \mapsto 0))$

(ОН) если $t=2$, то $\varkappa(pt) = \sup(\varkappa(p), (a \mapsto 0))$

(II) если $t=3$, то $\varkappa(pt) = \sup(\varkappa(p), (a \mapsto 1, b \mapsto 1))$

(OI) если $t=4$, то $\varkappa(pt) = \sup(\varkappa(p), (a \mapsto 0, b \mapsto 1))$

(IO) если $t=5$, то $\varkappa(pt) = \sup(\varkappa(p), (a \mapsto 1, b \mapsto 0))$

Объект $\varkappa(p)$ мы будем называть кандидатом вершины p.

Напомним, что априорная вероятность $P(A)$ множества A (точнее, задачи $\langle \Xi, A \rangle$) равна по определению $\mu(\{\omega | f(\omega) \in A\})$, где f – некоторый вычислимый объект пространства $C(\Omega, \Xi)$. Рассмотрим вычислимую возрастающую последовательность конечных объектов $f_0 \leq f_1 \leq \ldots$ пространства $C(\Omega, \Xi)$, для которой $\sup\{f_i | i \in N\} = f$ (такая последовательность существует в силу вычислимости f). Рассмотрим соответствующую последовательность мер $P_i(A) = \mu(\{\omega | f_i(\omega) \in A\})$. Легко проверить, что если x – конечный объект пространства Ξ, то $i \longmapsto P_i(\Gamma_x)$ – вычислимая возрастающая последовательность рациональных чисел, предел которой равен $P(\Gamma_x)$. В соответветствии с нашей интерпретацией процесса выбора мер μ_k как происходящего во времени, мы будем называть число $P_i(\Gamma_x)$ такущим значением априорной вероятности множества Γ_x в момент времени i (=на шаге i).

Процесс построения происходит по шагам. В конце каждого шага каждая вершина $\{1,2,3,4,5\}$-дерева находится в одином из трех состояний 0,1,2. Состояние вершины p определяет, чему равна (на этом шаге) мера $\mu_{N(p)}$: если состояние равно s, то мера $\mu_{N(p)}$ совпадает с мерой μ^s. Кроме того, в конце i-го шага выделено некоторое поддерево в $\{1,2,3,4,5\}$- дереве; вершины, в него входящие, мы будем называть активными (на данном шаге). Состояния вершин в конце i-го шага используются при выполнении $i+1$-го шага. Описывая $i+1$-ый шаг, мы будем называть состояние вершины p после i-го шага предыдущим состоянием вершины p, а состояние вершины p после $i+1$-го шага – новым состоянием вершины p. Напомним также, что значения меры P_i мы будем называть текущими значениями априорной вероятности.

Итак, мы описываем, как определяются состояния и активность вершин на $i+1$-ом шаге. Этот процесс идет снизу вверх, начиная с корня, который мы будем считатать по определению активной вершиной. Итак, пусть уже выяснено, является ли вершина p активной. Покажем, как выбирается (новое) состояние вершины p и какие из следующих за p вершин считаются активными (на данном шаге).

А. Пусть вершина p неактивна. Тогда ее состояние остается тем же, каким было на предыдущем шаге. Все следующие за ней вершины также объявим неактивными.

Б. Пусть вершина p активна и является вершиной уровня n (уровень вершины - длина соответствующего слова в алфавите $\{1,2,3,4,5\}$). Ее состояние и активность следующих за ней вершин определяется по таким правилам.

Б.0. Пусть предыдущее состояние вершины p было равно 0. В этом случае мы должны найти текущее значение априорной вероятности множеств $\Gamma_{\varkappa(p1)}$ и $\Gamma_{\varkappa(p2)}$ и сравнить их со значением $(\frac{2}{5})^{n+1}$. сли хотя бы одно из них не превышает этого значения, то состояние вершины p остается равным 0 и активными будут те из вершин $p1$ и $p2$, для которых априорные вероятности (точнее, текущие их значения) соответсвующих множеств $\Gamma_{\varkappa(p1)}$ и $\Gamma_{\varkappa(p2)}$ не превышают $(\frac{2}{5})^{n+1}$.

Пусть теперь текуюшие значения априорной вероятности множеств $\Gamma_{\varkappa(p1)}$ и $\Gamma_{\varkappa(p2)}$ превышают $(\frac{2}{5})^{n+1}$. Найдем текущее значение q априорной вероятности их пересечения $\Gamma_{\varkappa(p1)} \cap \Gamma_{\varkappa(p2)}$ и сравним его с $q_0 = \frac{1}{5} \cdot (\frac{2}{5})^n$

Если $q \le q_0$, то новое состояние вершины p будет равно 1, а из непосредственно следующих за p вершин активной будет вершина $p3$.

Если же $q > q_0$, то новое состояние вершины p будет равно 2, а активными будут те из вершин pi (i =4,5) для которых текущее значение априорной вероятности множества $\Gamma_{\varkappa(pi)}$ не превосходит $\left(\frac{2}{5}\right)^{n+1}$.

Б.I. Пусть предыдущее состояние вершины p было равно I. Тогда ее новое состояние также будет равно I и из непосредственно следующих за p вершин активной будет вершина $p3$.

Б.2. Пусть предыдущее состояние вершины p было равно 2. Тогда ее новое состояние также будет равно 2, а активными будут те из вершин pi , для которых $i \in \{4,5\}$ и текущее значение априорной вероятности множества $\Gamma_{\varkappa(pi)}$ не больше $\left(\frac{2}{5}\right)^{n+1}$.

Итак, определение новых состояний и поддерева активных вершин закончено. Установим теперь некоторые свойства изложенной конструкции.

Лемма 4. Если состояние вершины p уровня n в конце шага $i+1$ равно 2, то текущее значение априорной вероятности множества $\Gamma_{\varkappa(p1)} \cap \Gamma_{\varkappa(p2)}$ на этом шаге (то есть $P_i(\Gamma_{\varkappa(p1)} \cap \Gamma_{\varkappa(p2)})$) не меньше $\frac{1}{5} \cdot \left(\frac{2}{5}\right)^{n+1}$

Доказательство. Рассуждая по индукции, можно считать, что для меньших значений i утверждение леммы уже доказано. Если в конце шага i состояние вершины p было равно 2, то утверждение леммы следует из предположения индукции и монотонности $P_i(\Gamma_x)$ по i . Если в конце шага i состояние вершины p было отлично от 2, то оно было равно 0 (т.к. состояние I, раз появившись, сохраняется в дальнейшем, см.Б.I) и на шаге $i+1$ применялось правило Б.0. В этом случае утверждение леммы очевидно. ▨

Лемма 5. Если состояние вершины p уровня n в конце шага $i+1$ равно I, то текущее значение априорной вероятности множества $\Gamma_{\varkappa(p1)} \cup \Gamma_{\varkappa(p2)}$ на этом шаге (то есть $P_i(\Gamma_{\varkappa(p1)} \cup \Gamma_{\varkappa(p2)})$) не меньше $\frac{3}{5}\cdot\left(\frac{2}{5}\right)^n$

Доказательство проводится аналогично доказательству предыдущей леммы. Нужно заметить лишь, что из неравенств

$$P_i(\Gamma_{\varkappa(p1)}) \geq \frac{2}{5}\cdot\left(\frac{2}{5}\right)^n,\ P_i(\Gamma_{\varkappa(p2)}) \geq \frac{2}{5}\cdot\left(\frac{2}{5}\right)^n,$$

$P_i(\Gamma_{\varkappa(p1)} \cap \Gamma_{\varkappa(p2)}) \leq \frac{1}{5}\cdot\left(\frac{2}{5}\right)^n$ с учетом того, что $P(A\cup B) = P(A)+P(B)-P(A\cap B)$ вытекает неравенство

$$P_i(\Gamma_{\varkappa(p1)} \cup \Gamma_{\varkappa(p2)}) \geq \left(\frac{2}{5}+\frac{2}{5}-\frac{1}{5}\right)\cdot\left(\frac{2}{5}\right)^n. \ \boxtimes$$

Лемма 6. Если в конце шага $i+1$ вершина p уровня n активна, то текущее значение априорной вероятности множества $\Gamma_{\varkappa(p)}$ (то есть $P_i(\Gamma_{\varkappa(p)})$) не превосходит $\left(\frac{2}{5}\right)^n$.

Доказательство проводится индукцией по n . При $n=0$ утверждение очевидно. Пусть для вершин уровня n оно уже доказано и pt – активная вершина уровня $n+1$. Тогда предыдущая вершина (т.е. p) также активна и

$P_i(\Gamma_{\varkappa(p)}) \leq \left(\frac{2}{5}\right)^n$ по предположению индукции. Рассмотрим теперь возможные значения состояния вершины p в конце предыдущего, i -го, шага.

Пусть состояние вершины p к концу i -го шага было равно 2. Тогда утверждение леммы очевидно следует из построения (см. Б.2).

Пусть состояние вершины p к концу i -го шага было равно I. В этом случае $t=3$ и надо доказать, что

$P_i(\Gamma_{\varkappa(p3)}) \leq \left(\frac{2}{5}\right)^{n+1}$. Согласно лемме 5,

$P_i(\Gamma_{\varkappa(p1)} \cup \Gamma_{\varkappa(p2)}) \geq \frac{3}{5}\cdot\left(\frac{2}{5}\right)^n$. Но множества $\Gamma_{\varkappa(p1)} \cup \Gamma_{\varkappa(p2)}$ и $\Gamma_{\varkappa(p3)}$ не пересекаются и содержатся в множестве $\Gamma_{\varkappa(p)}$,

априорная вероятность которого (точнее, ее текущее значение) не превосходит $\left(\frac{2}{5}\right)^n$ по предположению индукции. Поэтому $P_i(\Gamma_{\varkappa(p3)}) \geq \left(\frac{2}{5}\right)^n - \frac{3}{5}\cdot\left(\frac{2}{5}\right)^n = \left(\frac{2}{5}\right)^{n+1}$.

Пусть теперь состояние вершины p к концу i-го шага было равно 0. Если текущее значение априорной вероятности одного из множеств $\Gamma_{\varkappa(p1)}$ и $\Gamma_{\varkappa(p2)}$ при выполнении $i+1$-го шага не превосходило $\left(\frac{2}{5}\right)^{n+1}$, то утверждение леммы очевидно. Если это не так, а априорная вероятность их пересечения превосходила $\frac{1}{5}\cdot\left(\frac{2}{5}\right)^n$, то новое состояние равно I, $t=3$,

$$P_i(\Gamma_{\varkappa(p1)} \cup \Gamma_{\varkappa(p2)}) \geq \left(\frac{2}{5}+\frac{2}{5}-\frac{1}{5}\right)\cdot\left(\frac{2}{5}\right)^n,$$

$$P_i(\Gamma_{\varkappa(p3)}) \leq \left(\frac{2}{5}\right)^n - \frac{3}{5}\cdot\left(\frac{2}{5}\right)^n = \left(\frac{2}{5}\right)^{n+1}$$

(ср. аналогичное рассуждение при доказательстве леммы 5). Если же априорная вероятность пересечения (точнее, ее текущее значение) превосходила $\frac{1}{5}\cdot\left(\frac{2}{5}\right)^n$, то утверждение леммы 6 очевидно выполнено (см. Б.I). Лемма 6 доказана.

Лемма 7. Если в конце $i+1$-го шага вершина p активна, то одна из непосредственно следующих за ней вершин (т.е. одна из вершин pt при $t\in\{\text{I},2,3,4,5\}$) активна в конце $i+1$-го шага.

Доказательство. Рассмотрим состояние вершины p в конце i-го шага. Если оно было равно I, то вершина $p3$ будет активной (см. Б.I). Пусть оно было равно 0. Из возможных при этом случаев требует разбора лишь случай, в котором текущие значения априорной вероятности множеств $\Gamma_{\varkappa(p1)}$ и $\Gamma_{\varkappa(p2)}$ превышают $\frac{2}{5}\cdot\left(\frac{2}{5}\right)^n$, а текущее значение априорной вероятности их пересечения превышает $\frac{1}{5}\cdot\left(\frac{2}{5}\right)^n$. Заметим, что множества $\Gamma_{\varkappa(p1)}\cap\Gamma_{\varkappa(p2)}$, $\Gamma_{\varkappa(p4)}$, $\Gamma_{\varkappa(p5)}$ попарно не пересекаются и содержатся в множестве $\Gamma_{\varkappa(p)}$, текущее значение априорной вероятности которого не превосходит $\left(\frac{2}{5}\right)^n$ по лемме 6. Раз текущее значение априорной вероятности пересечения

$\Gamma_{\varkappa(p1)} \cap \Gamma_{\varkappa(p2)}$ превосходит $\frac{1}{5}\cdot\left(\frac{2}{5}\right)^n$, то сумма текущих значений априорной вероятности множеств $\Gamma_{\varkappa(p4)}$ и $\Gamma_{\varkappa(p5)}$ не превосходит $\frac{4}{5}\cdot\left(\frac{2}{5}\right)^n$, и, значит, одна из вершин $p4$ и $p5$ активна.

Аналогичным образом с использованием лемм 4 и 6 рассматривается случай, в котором состояние вершины p в конце i -го шага было равно 2. Лемма 7 доказана. ▨

Следствие леммы 7. В конце каждого шага построения существуют активные вершины всех уровней. ▨

Лемма 8. Если вершина p уровня n активна в конце i -го шага, то мера R_i (определяемая, напомним, состояниями вершин в конце этого шага) множества $\Gamma_{\varkappa(p)}$ равна $\left(\frac{1}{2}\right)^n$.

Доказательство. Напомним, что мера R_i определяется как произведение мер μ_s на $\mathcal{U}_s$, где каждая из мер μ_s равна μ^0, μ^1 или μ^2 в зависимости от состояния соответствующей вершины (состояние вершины p определяет меру $\mu_{N(p)}$). Пусть $p = p_0 \ldots p_{n-1}$. Тогда $\Gamma_{\varkappa(p)}$ есть произведение множеств $V_s \subset \mathcal{U}_s$, причем все V_s, за исключением тех, у которых $s \in \{N(p_0), N(p_0 p_1), \ldots, N(p_0 \ldots p_{n-2})\}$, будут совпадать с $\mathcal{U}_s$, а $V_{N(p_0 \ldots p_t)}$ будет совпадать с одним из множеств

{Н0,00,I0}	(если	$p_{t+1} = 1$)
{0Н,00,0I}	(если	$p_{t+1} = 2$)
{II}	(если	$p_{t+1} = 3$)
{0I}	(если	$p_{t+1} = 4$)
{I0}	(если	$p_{t+1} = 5$)

Мера на $\mathcal{U}_{N(p_0 \ldots p_t)}$ зависит от состояния вершины $p_0 \ldots p_t$,

которое (т.к. вершина $p_0 \dots p_n$ активна) определяется значением p_{t+1}. В самом деле, из построения легко следует, что если в конце i-го шага вершина $p\alpha$ активна, то при $\alpha = 1$ или $\alpha = 2$ состояние вершины p равно 0, при $\alpha = 3$ оно равно I, при $\alpha = 4$ или $\alpha = 5$ оно равно 2. Теперь ясно, что имеющаяся в сомножителе $\mathcal{U}_{N(p_0 \dots p_t)}$ мера множества $V_{N(p_0 \dots p_t)}$ будет равна I/2. Таким образом, мера множества $\Gamma_{\varkappa(p)}$ будет равна $(I/2)^n$. Лемма 8 доказана. ▨

Теперь можно завершить доказательство предложения 5, установив, что для любой константы $C > 0$ найдется такое множество A, что $P(A) < \frac{R(A)}{C}$.

В самом деле, возьмем достаточно большое n и вершину p уровня n, которая на бесконечном числе шагов нашего построения является активной (такая существует, так как на каждом шаге есть активная вершина уровня n, а всего вершин уровня n конечное число). Для шагов i, на которых она активна, имеем (при $A = \Gamma_{\varkappa(p)}$):

$$P_i(A) \leq \left(\frac{2}{5}\right)^n, \quad R_i(A) = \left(\frac{1}{2}\right)^n,$$

и, следовательно, $P_i(A) / R_i(A) \leq \left(\frac{4}{5}\right)^n$. Переходя к пределу при $i \to \infty$ (по тем значениям i, для которых p активна), мы видим, что $P(A) / R(A) \leq \left(\frac{4}{5}\right)^n$.

Так как число n может быть выбрано сколь угодно большим, отношение $\frac{P(A)}{R(A)}$ может быть сделано сколь угодно малым. Доказательство предложения 5 закончено. ▨

4.4. Логарифм априорной вероятности и энтропия.

Априорную вероятность задачи можно рассматривать как характеризацию степени трудности её решения: чем априорная вероятность меньше, тем задача труднее. Удобно перейти к двоичным логарифмам, сопоставив каждой задаче α величину

$$KP(\alpha) = -\log_2 P(\alpha)$$

где $P(\alpha)$ - априорная вероятность задачи α. Теперь можно сказать, что чем $KP(\alpha)$ больше, тем задача α труднее.

В этом пункте мы сравниваем величину KP с другими видами энтропии.

Предложение I. Пусть X - произвольное пространство. Существует такая константа C, что для любой монотонной задачи α в пространстве X справедливо неравенство

$$KP(\alpha) \leq K_\Omega(\alpha) + C.$$

Доказательство. Пусть $f \in C(\Omega, X)$ - оптимальный способ описания (способ, при котором K_f минимальна). Пусть $K_\Omega(\alpha) = K_f(\alpha) = n$. Тогда существует $x \in \Omega^*$, для которого $l(x) = n$ и $f(x)$ - решение задачи α. Пусть ω - произвольная бесконечная последовательность нулей и единиц, начинающаяся на x. Тогда $f(\omega) \geq f(x)$ и (в силу монотонности задачи α) $f(\omega)$ является решением задачи α. Поэтому множество $\{\omega \in \Omega \setminus \Omega^* \mid f(\omega) - \text{решение } \alpha\}$ содержит Γ_x и его мера не меньше 2^{-n}. Поэтому $P_f(\alpha) \geq 2^{-n}$ и $P(\alpha) \geq 2^{-n} \cdot c$, где c - положительная константа, зависящая только от пространства X (но не от задачи α). Отсюда $KP(\alpha) \leq n + c'$ (где $c' = -\log_2 c$) и тем самым $KP(\alpha) \leq K_\Omega(\alpha) + c'$. Предложение I доказано. ▨

Нас будет интересовать вопрос о том, при каких условиях выполняется неравенство, обратное к неравенству предложения I (или его аналоги).

Ограничимся сначала случаем, в котором $\alpha = \langle X, \Gamma_x \rangle$ где x – некоторый конечный объект пространства X. Как доказано в [2, теорема 2.3], при $X = \mathbb{N}_\perp$, $\alpha = \langle X, \Gamma_x \rangle$ величины $KP(\alpha)$ и $K_\Omega(\alpha)$ отличаются на ограниченное слагаемое. Этот факт является специфическим свойством пространства $\mathbb{N}_\perp$. Как видно из предложения 2, для пространства Ξ и задач вида $\langle \Xi, \Gamma_x \rangle$ аналогичное утверждение не выполняется. В работе П.Гача [17] установлено (значительно более сложным образом), что аналогичное утверждение не выполняется и для пространства Ω.

Предложение 2. Не существует такой константы C, что для любого конечного объекта x пространства Ξ выполнено неравенство $K_\Omega(\langle \Xi, \Gamma_x \rangle) \leq KP(\langle \Xi, \Gamma_x \rangle) + C$.

Доказательство. Заметим прежде всего, что

$$\exists C_1 (\forall x \in \Xi) \ (KP(\langle \Xi, \Gamma_x \rangle) \leq \ell(x) + C_1)$$

В самом деле, рассмотрим способ описания $f \in C(\Omega, \Xi)$, сопоставляющий с последовательностью $x_0 x_1 \ldots$ функцию t, для которой $t(0) = x_0$, $t(1) = x_1$ и т.д. Легко видеть, что мера множества тех бесконечных последовательностей $\omega \in \Omega$ для которых $f(\omega) \in \Gamma_x$, равна $2^{-\ell(x)}$ (при любом конечном $x \in \Xi$), так как условие $f(\omega) \in \Gamma_x$ фиксирует $\ell(x)$ членов последовательности ω. Поэтому

$$P_f(\langle \Xi, \Gamma_x \rangle) = 2^{-\ell(x)}, \ P(\langle \Xi, \Gamma_x \rangle) \geq C_2 \cdot 2^{-\ell(x)},$$

$KP(\langle \Xi, \Gamma_x \rangle) \leq \ell(x) + C_1$. Осталось доказать, что ни при каком C не может быть выполнено (для любого x) неравенство $K_\Omega(\langle \Xi, \Gamma_x \rangle) \leq \ell(x) + C$. Но это доказано нами в п. 2.5 (предложение 3). Предложение 2 доказано. ▨

Покажем теперь, что положение можно исправить, заменив пространство Ω на другое регулярное пространство с объемом.

Предложение 3. Существует такое регулярное пространство с объемом $\langle M, \ell \rangle$, что для любого пространства X существует такая константа C, что для любого конечного объекта x пространства X выполнено неравенство

$$|KP(\langle X, \Gamma_x \rangle) - K_{\langle M, \ell \rangle}(\langle X, \Gamma_x \rangle)| \leq C.$$

Это предложение показывает, что если интересоваться лишь задачами вида $\langle X, \Gamma_x \rangle$, то логарифм априорной вероятности может рассматриваться как один из видов энтропии.

Доказательство предложения 3. Построим пространство M и объем ℓ. Конечными объектами пространства будут конечные множества двоичных слов, ни одно из которых не является началом другого. В п. 4.3 такие множества были названы наборами. (Нам потребуются также некоторые связанные с наборами понятия. Они введены в п. 4.3 при доказательстве леммы I.) Введем частичный порядок на наборах, считая, что $x \leq y$, если набор x шире набора y. (Заметим, что введенное так отношение порядка обратно рассматривавшемуся в п. 4.3.) Чтобы построить пространство, конечными объектами которого будут наборы с введенным таким образом порядком, нужно, согласно п. I.3, проверить, что имеется наименьший объект и что любые два совместных объекта имеют точную верхнюю грань. Наименьшим объектом будет набор, единственным элементом которого является пустое слово. Пусть теперь объекты x и y совместны. Это означает, что имеется набор w, для которого $x \leq w$ и $y \leq w$, то есть x шире w и y шире w. Покажем, что объекты x и y име-

ют точную верхнюю грань. Пусть $x = \{x_1, \ldots, x_m\}$, $y = \{y_1, \ldots, y_n\}$. Рассмотрим все пары $\langle x_i, y_j \rangle$, для которых x_i и y_j совместны (т.е. одно из них продолжает другое). (Такие пары найдутся, так как любой элемент набора w является продолжением некоторого x_i и некоторого y_j.) Для всякой такой пары включим в z более длинный из ее членов. Очевидно, $x \leq z$ и $y \leq z$. Пусть z' – любой набор, для которого $x \leq z'$ и $y \leq z'$. Покажем, что $z \leq z'$. Если t – любое слово из z', то (по определению отношения порядка) найдутся $x_i \in x$ и $y_j \in y$, являющиеся началами t. Но тогда наибольшее из слов x_i и y_j входит в z.

Итак, согласно п. I.3, множество всех наборов можно считать множеством конечных объектов некоторого пространства. Это пространство мы обозначим через M. Осталось ввести на M объем. Напомним, что в п. 4.3 каждому набору x было сопоставлено число $|x|$, названное его мерой. Объемом набора x мы будем считать целую часть числа $-\log_2 |x|$. Очевидно, так определенная функция удовлетворяет всем требованиям, предъявляемым к объемам.

Итак, пространство с объемом $\langle M, \ell \rangle$ построено. Надо показать, что оно является регулярным. Для этого построим отображение $f \in C(M, M \times \mathbb{N}_\perp)$, при котором

$$K_f(\langle M \times \mathbb{N}_\perp, \{\langle m, n \rangle\} \rangle) \leq \ell(m) + C(n)$$

где $C(n)$ – некоторая функция, зависящая только от n. Функцию f определим так. Пусть m – произвольный набор. Будем искать такое $n \in \mathbb{N}$, что все слова из m начинаются на $0^n 1$. Если такого n нет, то положим $f(m) = \perp$. Если такое n существует, то оно единственно. Возьмем в качестве $f(m)$ пару $\langle m', n \rangle$, где

m' – набор, получающийся из набора m отбрасыванием начала $0^n 1$ во всех его члена. На бесконечные объекты пространства M функция f продолжается по непрерывности, при этом используется лемма 5 из п. I.4.3.3. Легко понять, что f – непрерывное вычислимое отображение и для конечных объектов $m \in M$ имеет место равенство $|m'| = 2^{n+1} \cdot |m|$. Отсюда следует написанное выше неравенство для $K_f(\langle M \times \mathbb{N}_\perp, \{\langle m, n\rangle\}\rangle)$.

Регулярность пространства $\langle M, \ell\rangle$ доказана. Покажем теперь, что $KP(\langle X, \Gamma_x\rangle) = K_{\langle M, \ell\rangle}(\langle X, \Gamma_x\rangle) + O(1)$.

Пусть $f \in C(M, X)$ – оптимальный способ описания. Определим способ описания $f^* \in C(\Omega, X)$, положив $f^*(t)$ для конечных $t \in \Omega$ равным $f(\{t\})$ (значению f на наборе, единственным элементом которого является t). На бесконечные последовательности f^* продолжается по непрерывности (п. I.4.3.3, лемма 5). Покажем, что

$$P_{f^*}(\langle X, A\rangle) \geq 2^{-K_f(\langle X, A\rangle) - 1}$$

для любой монотонной задачи $\alpha = \langle X, A\rangle$. В самом деле, пусть набор $m = \{x_1, \dots, x_k\}$ является описанием решения задачи α (то есть $f(m) \in A$), причем $\ell(m) = K_f(\alpha)$. Тогда $f(\{x_1\}), \dots, f(\{x_k\})$ также принадлежат A, так как $\{x_i\} \geq \{x_1, \dots, x_k\}$ в пространстве M, а задача A монотонна. Отсюда следует, что для любой бесконечной последовательности ω, начинающейся на одно из слов $x_1, \dots, x_k$, выполняется соотношение $f^*(\omega) \in A$, и, следовательно, $P_{f^*}(\langle X, A\rangle)$ не меньше меры набора m. Поэтому $P_{f^*}(\langle X, A\rangle) \geq 2^{-\ell(m) - 1}$ (-1 появляется, так как при определении ℓ мы брали целую часть от логарифма меры). Из доказанного следует, что

$$KP(\langle X, \Gamma_x \rangle) \leq K_{\langle M, \ell \rangle}(\langle X, \Gamma_x \rangle) + \mathcal{O}(1).$$

Докажем теперь обратное неравенство. Пусть $f \in C(\Omega, X)$ – оптимальный способ описания (тот, при котором вероятность задач наибольшая). Построим $F \in C(M, X)$, определив значение его на конечных объектах пространства M так: для любого набора $\{a_1, \ldots, a_k\}$ выполнено равенство $F(\{a_1, \ldots, a_k\}) = \sup\{x \mid x$ – конечный объект, $x \leq f(a_1), \ldots, x \leq f(a_k)\}$ (верхняя грань в правой части определена в силу леммы 3 из п. I.3). Для определения значений F на бесконечных объектах мы воспользуемся, как и раньше, леммой 5 из п. I.4.3.3; необходимая для этого монотонность F легко проверяется. Покажем теперь, что

$$K_F(\langle X, \Gamma_x \rangle) \leq -\log_2 P_f(\langle X, \Gamma_x \rangle)$$

(Это завершит доказательство предложения 3.) Пусть $P_f(\langle X, \Gamma_x \rangle) = \alpha$. Другими словами, мера открытого множества $\{\omega \in \Omega \setminus \Omega^* \mid f(\omega) \geq x\}$ равна α. Поэтому можно найти набор $m = \{a_1, \ldots, a_k\}$, для которого $f(a_1) \geq x, \ldots, f(a_k) \geq x$ и мера которого сколь угодно близка к α. Для этого набора m имеет место неравенство $F(m) \geq x$ и, следовательно,

$$K_F(\langle X, \Gamma_x \rangle) \leq \ell(m) \leq -\log_2(|m|)$$

Так как мера набора m может быть сколь угодно близка к α, получаем, что $K_F(\langle X, \Gamma_x \rangle) \leq -\log_2 \alpha = KP(\langle X, \Gamma_x \rangle)$. Предложение 3 доказано. ▨

Покажем теперь, что ограничение класса рассматриваемых в предложении 3 задач задачами вида $\langle X, \Gamma_x \rangle$ существенно.

Предложение 4. Не существует такого регулярного пространства с объемом $\langle M, \ell \rangle$, что для любого пространства X существует такая константа C, что для любой монотонной задачи α в пространстве X выполнено неравенство

$$|KP(\alpha) - K_{\langle M, \ell \rangle}(\alpha)| \leq C.$$

Доказательство. Пусть такое пространство $\langle M, \ell \rangle$ существует. Возьмем в качестве X пространство Ω, а в качестве α – задачу $\langle \Omega, S \rangle$, где S – множество всех (бесконечных) невычислимых последовательностей нулей и единиц. Легко видеть, что мера множества S равна 1, поэтому при тождественном способе описания $f \in C(\Omega, \Omega)$ имеет место равенство $P_f(\alpha) = 1$. Поэтому $KP(\alpha)$ конечна. С другой стороны, $K_{\langle M, \ell \rangle}(\alpha) = \infty$. В самом деле, пусть $g \in C(M, \Omega)$ – оптимальный способ описания. Легко видеть, что ни для какого конечного объекта $x \in M$ значение $g(x)$ не будет решением задачи α, так как $g(x)$ – вычислимый объект пространства Ω (согласно лемме 3 из п. I.5.3, результат применения вычислимого объекта к вычислимому – и тем более к конечному – вычислим). Предложение 4 доказано. ▨

4.5. Аксиоматическое описание энтропии.

В этом пункте мы исследуем возможность задания энтропии с помощью перечисления её свойств.

Пусть E – произвольная всюду определенная функция из $\mathbb{N}$ в $\mathbb{N}$. Сформулируем три требования, накладываемых на функцию E.

(I) По n можно эффективно указать номер перечислимого множества, состоящего из всех чисел x, для которых $E(x)$ не превосходит n.

Эквивалентная формулировка: E является пределом вычислимой убывающей последовательности всюду определенных вычислимых функций. (В самом деле, если $E = \lim E_p$ и $E_p(x) \geqslant E_{p+1}(x)$ при всех p и x, то

$$\{x \mid E(x) \leq n\} = \bigcup_p \{x \mid E_p(x) \leq n\}$$

Обратно, если $\{x \mid E(x) \leq n\}$ имеет номер $\varphi(n)$, то положив

$\widetilde{E}_0(x) = \min\{n \mid x$ появляется после n шагов перечисления множества с номером $\varphi(i)$ при некотором $i \leq n\}$

и

$\widetilde{E}_p(x) = \min(\{\widetilde{E}_0(x)\} \cup \{n \mid x$ появляется после выполнения p шагов перечисления множества с номером $\varphi(n)\})$,

мы получаем убывающую последовательность вычислимых функций, сходящуюся к E.)

Требование (I) гарантирует, что если значение E на некотором объекте мало, то рано или поздно это обстоятельство обнаружится.

Подсчитаем количество объектов (=чисел) x, для которых $E(x)$ не превосходит n. Обозначим это число $e(n)$.

Второе требование состоит в том, что $e(n)$ отличается от 2^n не более чем на мультипликативную константу:

(2) Существуют такие C_1, $C_2 > 0$, что для всех имеет место неравенство

$$C_1 \cdot 2^n \leq e(n) \leq C_2 \cdot 2^n.$$

Переходя к логарифмам, требование (2) можно, очевидно, переписать так:

$$\exists C \, \forall n \quad |\log_2 e(n) - n| \leq C$$

Третье требование, накладываемое на функцию E, гласит:

(3) для любой вычислимой функции f из $\mathbb{N}$ в $\mathbb{N}$ найдется такая константа C, что при всех выполнено неравенство

$$E(f(x)) \leq E(x) + C.$$

Оно гарантирует, что при алгоритмическом преобразовании объектов значение функции E не может неограниченно расти.

Легко видеть, что взяв в качестве E простую колмогоровскую энтропию, мы удовлетворим всем трем требованиям. Оказывается, что сформулированные требования однозначно определяют функцию E (с точностью до ограниченного слагаемого). Именно, имеет место

Теорема I. Пусть всюду определенная функция $E : \mathbb{N} \to \mathbb{N}$ удовлетворяет требованиям (I), (2) и (3). Тогда E отличается от простой колмогоровской энтропии K не более чем на константу:

$$\exists C \, \forall x \quad (|E(x) - K(x)| \leq C)$$

(Напомним, что через $K(x)$ мы обозначаем простую колмогоровскую энтропию объекта x.)

Доказательство. Пусть функция E удовлетворяет требованиями (I), (2) и (3). Докажем сначала, что при некотором C выполнено неравенство

$$K(x) \leq E(x) + C$$

(при всех x). [При этом не будет использовано то, что функция удовлетворяет требованию (3).]

Согласно требованию (2), найдется такое A, что количество объектов x с $E(x) \leq n$ не превосходит $A \cdot 2^n$. Построим способ описания (т.е. вычислимую частичную функцию из $\mathbb{N}$ в $\mathbb{N}$, сопоставляющую описанию описываемый объект, см. п. 4.I), отведя для объектов с $E(x) \leq n$ участок натурального ряда длиной $A \cdot 2^n$ и заполняя его по мере появления таких объектов. Более точно, разобьем натуральный ряд на участки длиной A, $2A$, $4A, \ldots,$ следующие друг за другом, и через $r(n,k)$ обозначим k-ое по порядку число участка длиной $2^n A$. Перечисляя множество всех объектов x с $E(x) \leq n$, будем снабжать эти объекты описаниями, считая $r(n,i)$ описанием i-го (в порядке появления при перечислении) объекта этого множества. В силу наших предположений это возможно (описаний не меньше, чем объектов) и получающийся способ описания вычислим в силу требования (I). При этом для всякого объекта x, для которого $E(x) \leq n$ найдется описание, не превосходящее $A \cdot 2^{n+1}$ (так как $1 + 2 + \ldots + 2^n \leq 2^{n+1}$); его объем, очевидно, не превосходит $n + \log_2 A + 1$. Поэтому

$$K(x) \leq E(x) + O(1).$$

Перейдем теперь к доказательству обратного неравенства. Согласно (2), число объектов x с $E(x) \leq n$ не меньше 2^{n-c} при некотором c . Будем составлять для каждого

$n \geq C$ список объектов x с $E(x) \leq n$, прекращая его составление в тот момент, когда число объектов списка сравняется с 2^{n-C}. Так как выполнено требование (I), этот процесс можно выполнять эффективно и получить вычислимую последовательность конечных множеств

$$B_C\,,\ B_{C+1}\,,\ \ldots$$

со следующими свойствами:

(а) для всякого $x \in B_k$ значение $E(x)$ не превосходит k ;

(б) число элементов $B_k = 2^{k-C}$.

Не ограничивая общности, можно считать, что

(в) $B_k \subset B_{k+1}$ при всех k .

(В самом деле, если это не так, можно изменить множества B_0, B_1,..., добавив все элементы B_k в B_{k+1} и исключив лишние – с тем, чтобы схоранить (а) и (б).)

Построим теперь вычислимую функцию $f: \mathbb{N} \to \mathbb{N}$, которая, суженная на B_{C+i}, осуществляет взаимно однозначное соответствие между этим множеством и множеством $\{0, 1, \ldots, 2^i - 1\}$:

B_C B_{C+1} B_{C+2}

0 1 2 3 4

Так как функция E удовлетворяет требованию (3), то выполнено неравенство

$$E(f(x)) \leq E(x) + O(1)$$

Таким образом, для $x \in \{0, 1, \ldots, 2^i - 1\}$ имеем

$$E(x) \leq i + C + O(1) = i + O(1).$$

Отсюда видно, что

$$E(x) \leq \log_2 x + O(1).$$

Пусть теперь $F : \mathbb{N} \to \mathbb{N}$ – оптимальный способ описания. Применяя еще раз (3), получаем, что $E(F(t)) \leq E(t) + O(1)$. Если x – произвольный объект, а t – его описание наименьшего объема, то

$$E(x) \leq E(t) + O(1) \leq \log_2 t + O(1) = K(x) + O(1),$$

что и требовалось доказать. Теорема I доказана.

Применим теперь теорему I к исследованию энтропий на пространстве $\mathbb{N}_\perp$,возникающих при различных пространствах описаний. Пусть X – произвольное регулярное пространство с объемом. Через $K_X(n)$ обозначим $K_X(\langle \mathbb{N}_\perp, \{n\} \rangle)$. Имеет место следующее

Предложение I. Функция K_X при любом регулярном X удовлетворяет требованиям (I) и (3).

Доказательство. Выполнение требования 3 очевидно следует из результатов п. 2.6. Проверим выполнение требования (I). Согласно определению,

$$K_X(n) = \min \{ l(p) \mid p \in X_0,\ n \leq F(p) \}$$

где F – оптимальный способ описания. (Отметим кстати, что неравенство $n \leq F(p)$ можно в рассматриваемом нами случае пространства $\mathbb{N}_\perp$ заменить на равенство $n = F(p)$.) В силу вычислимости F множество таких n и p , для которых $n \leq F(p)$, можно перечислить. (Точнее следовало бы говорить не о p , а об их номерах.) Отсюда и вытекает требование (I). Предложение I доказано.

Используя предложение I, можно получить из теоремы I такое

Следствие. Пусть X – произвольное регулярное пространство с объемом, причем количество объектов $x \in \mathbb{N}$, для которых $K_X(x) \leq n$, отличается от 2^n не более чем

аддитивную константу.

Поэтому, например, префиксная энтропия не удовлетворяет требованию (2). Однако она удовлетворяет более слабому требованию

$$(2') \quad \exists C_1 \exists C_2 \forall n \quad |\log_2 e(n) - n| \le C_1 + C_2 \log_2 n$$

Напомним, что $e(n)$ – число объектов x, для которых $E(x) \le n$. К таким видам энтропии применима следующая теорема.

<u>Теорема 2</u>. Пусть функция E обладает свойствами (I), (2'), (3). Тогда существуют такие C_1' и C_2', что для всех x выполнено неравенство

$$|E(x) - K(x)| \le C_1' + C_2' \log_2 l(x)$$

<u>Доказательство теоремы 2</u> проходит аналогично доказательству теоремы I с некоторыми изменениями. Отметим их. В первой части доказательства мы должны для объектов x с $E(x) \le n$ отвести участок натурального ряда длиной $A \cdot n^B \cdot 2^n$ при подходящих значениях A и B (можно взять $A = 2^{C_1}$, $B = C_2$) и соответствующим образом определить функцию τ. При этом для всякого объекта x, для которого $E(x) \le n$, найдется описание, не превосходящее

$$\sum_{i=1}^{n} A \cdot i^B \cdot 2^i$$

Как легко видеть, сумма не превосходит

$$O(1) \cdot A \cdot n^B \cdot 2^n$$

и её логарифм не превосходит

$$n + B \log_2 n + O(1)$$

что и гарантирует выполнение неравенства

$$K(x) \le E(x) + O(\log_2 E(x))$$

Если $K(x) \le E(x)$, то интересующее нас неравенство $K(x) \le E(x) + O(\log_2 l(x))$ очевидно выполнено; если же $K(x) > E(x)$, то $K(x) \le E(x) + O(\log_2 E(x)) \le$

$\leq E(x) + O(\log_2 K(x)) \leq E(x) + O(\log_2 \ell(x))$.

Во второй части доказательства число объектов x с $E(x) \leq n$ будет не меньше $2^{-n-c-c_1 \log n}$. Дальнейшие построения приводят к последовательности множеств B_i (определенных при всех достаточно больших i), обладающих свойствами (а) и (в) из доказательства теоремы I; свойство (б) заменяется на

(б′) $card\,(B_k) = [2^{k-c-c_1 \log_2 k}]$

(квадратные скобки обозначают целую часть). Рассуждая дальше, мы вместо неравенства $E(x) \leq \log_2 x + O(1)$ придем к неравенству $E(x) \leq k$ для всех $x \leq 2^{k-c-c_1 \log_2 k}$, откуда легко получить, что $E(x) \leq \log_2 x + O(\log_2 \log_2 x) + O(1)$. Далее доказательство теоремы 2 заканчивается аналогично доказательству теоремы I.

С помощью предложения I из теоремы 2 можно получить такое

Следствие. Пусть X – произвольное регулярное пространство с объемом, причем логарифм количества объектов $x \in \mathbb{N}$, для которых $K_X(x) \leq n$, отличается от n не более чем на $C_1 \log_2 n + C_2$. Тогда $K_X(x)$ отличается от простой колмогоровской энтропии не более чем на $O(\log_2 \ell(x))$.

4.6. Понятие (α, β)-стохастичности по Колмогорову и его свойства.

В этом пункте мы исследуем свойства введеного А.Н.Колмогоровым понятия стохастического конечного объекта. Говоря неформально, стохастические объекты – это объекты "общего положения" простых множеств. Приведем точные определения.

В качестве конечных объектов мы будем рассматривать натуральные числа. Напомним, что через $K(x)$ обозначается простая колмогоровская энтропия числа x. Нам потребуется говорить об энтропии конечных множеств натуральных чисел. Для этого мы фиксируем какую-либо естественную нумерацию конечных множеств (например, описанную в [11]) и под энтропией множества будем понимать энтропию его номера. Энтропия множества A будет обозначаться $K(A)$.

Определение (А.Н.Колмогоров). Пусть α, β – натуральные числа. Число x будем называть (α, β)-стохастическим, если существует такое конечное множество $A \subset \mathbb{N}$, что

$$x \in A, \quad K(A) \leq \alpha, \quad K(x) \geq \log_2 |A| - \beta;$$

здесь через $|A|$ обозначено число элементов множества A.

Первое неравенство (если α невелико) означает, что множество A достаточно просто. Второе (если β невелико) означает, что элемент x является элементом "общего положения" в множестве A. Действительно, если бы x обладал какими-нибудь особенностями, которые свойственны лишь очень малой части Q множества A, то их можно было бы использовать для простого описания x, указав его порядковый номер в списке всех элементов Q, что потребовало было $\log_2 |Q|$ бит, т.е. много меньше $\log_2 |A|$.

Установим связь понятия (α , β)-стохастичности с основаниями математической статистики. Пусть мы проводим некоторый вероятностный эксперимент, реузльтатом которого *a priori* может быть любое натуральное число. Пусть результатом этого эксперимента оказалось число x . Зная x , мы хотим восстановить распределение вероятностей P на множестве $\mathbb{N}$ всех натуральных чисел. Разумно требовать, чтобы, во-первых, P имело простое описание, а, во-вторых, x было бы "типичным" исходом опыта с распределением вероятностей P . (На практике специфика задачи часто заранее подсказывает возможный вид P и остается выбрать какие-то его параметры; мы, однако, считаем, что единственное имеющееся у нас сведение о P – это полученное значение x .)

Уточним сказанное. В качестве распределений вероятностей будем рассматривать всюду определенные функции $P:\mathbb{N}\to\mathbb{Q}$ все значения которых неотрицательны, $P(x)=0$ для всех x , кроме конечного числа, и $\sum_x P(x)\leq 1$. (Мы допускаем возможность $\sum P(x)<1$, считая, что наш эксперимент может и не дать результата.) Чтобы говорить об энтропии таких функций, фиксируем какую-нибудь естественную нумерацию их натуральными числами и, говоря об энтропии функции, будем иметь в виду (простую колмогоровскую) энтропию ее номера. Энтропию распределения P будем обозначать $K(P)$. Теперь требование простоты распределения P превращается в требование малости его энтропии. Требование "типичности" x для распределения P мы уточним так: $K(x)$ не должно быть много меньше $-\log_2 P(x)$. Если, например, P приписывает вероятность $1/2^n$ всем числам от 0 до 2^n-1 , то "типичными" будут те $x\in$

$\in \{0, 1, \ldots, 2^n - 1\}$, для которых энтропия $K(x)$ близка к n.

Отметим, что $K(x)$ не может сильно превосходить $-\log_2 P(x)$ если распределение P достаточно просто. Именно, при любом x справедливо неравенство

$$K(x) \leq -\log_2 P(x) + K(P) + O(\log_2(-\log_2 P(x) + K(P))).$$

В самом деле, пусть $1/2^{k+1} \leq P(x) \leq 1/2^k$. Рассмотрим множество всех t, для которых $P(t) \geq 1/2^{k+1}$. В нем не более 2^{k+1} элементов, и x – один из них. Чтобы задать x, достаточно указать это множество и порядковый номер элемента x в нем. Для указания множества достаточно указать P и число k; указание порядкового номера требует не более $k+1$ бит. Отсюда и вытекает написанное неравенство. Требование "типичности" x гарантирует, что это неравенство будет близко к равенству (если энтропия P невелика).

Определение. Пусть α, β – натуральные числа. Число x назовем (α, β)-квазистохастическим, если существует такое распределение P (из описанного класса), что

$$K(P) \leq \alpha, \quad K(x) \geq -\log_2 P(x) - \beta.$$

Понятия стохастичности и квазистохастичности оказываются весьма близкими. Именно, имеет место

Теорема I. Существуют такие константы C_1 и C_2, что для любого числа x:

а) если x является (α, β)-стохастическим, то является ($\alpha + C_1$, β)-квазистохастическим;

б) если x является (α, β)-квазистохастическим и $x \in \{0, 1, \ldots, 2^{n-1}\}$, то x является ($\alpha + C_1 \log_2 n$, $\beta + C_2$)-стохастическим.

Эта теорема показывает, что стохастичность и квазистохастичность "совпадают с точностью до $\log_2 n$".

Доказательство. Утверждение а) доказываетя легко. Пусть $x \in A$, (энтропия A) $\leqslant \alpha$, $K(x) \geqslant \log_2 |A| - \beta$. Рассмотрим распределение P, приписывающее всем элементам множества A одинаковые вероятности, равные $1/|A|$, и всем остальным числам – нулевые вероятности. Очевидно, энтропия P превосходит энтропию A не более, чем на константу, а $\log_2 |A| = -\log_2 P(x)$. Отсюда и получаем требуемое.

Чуть более сложно доказывается утверждение б). Пусть число x является (α, β)-квазистохастическим. Тогда существует такое распределение P, энтропия которого не превосходит α, а $K(x) \geqslant -\log_2 P(x) - \beta$. Пусть k – такое число, что $2^{-(k+1)} \leqslant P(x) \leqslant 2^{-k}$. Тогда $K(x) \geqslant k - \beta$. Из этого неравенства и из неравенства $K(x) \leqslant n + O(1)$ вытекает, что $k \leqslant n + \beta + O(1)$ (эта оценка потребуется нам в дальнейшем). Рассмотрим теперь множество A, состоящее из всех $y \in \mathbb{N}$, для которых $P(y) \geqslant 2^{-(k+1)}$. Чтобы задать A, достаточно указать P и указать k, поэтому энтропия A не превосходит $\alpha + C \log_2 (n + \beta)$. Множество A содержит не более 2^{k+1} элементов, поэтому $K(x) \geqslant \log_2 |A| - (\beta + 1)$. Таким образом, x является ($\alpha + C \log_2 (n+\beta)$, $\beta + 1$)-стохастическим. Если $\beta \leqslant n$, то утверждение п. б) доказано. Если же $\beta > n$, то любое число от 0 до $2^n - 1$ является ($C \log_2 n$, β)-стохастическим (достаточно в качестве A взять множество всех чисел от 0 до $2^n - 1$). Теорема 1 доказана.

Обратимся теперь к вопросу о том, при каких α и β среди чисел от 0 до 2^{n-1} существуют не (α, β)-стохастические. Ответ на этот вопрос дает

Теорема 2. а) Существует такое C, что при любом n и

любых α и β, для которых $\alpha \geq \log_2 n + C$, $\alpha+\beta \geq n + 4\log_2 n + C$, все числа от 0 до $2^n - 1$ являются (α, β)-стохастическими.

б) Существует такое C, что при любом n и любых α и β, для которых $2\alpha + \beta < n - 6\log_2 n - C$, не все числа от 0 до $2^n - 1$ являются (α, β)-стохастическими.

Доказательство. а) Пусть сначала $\beta \leq n$. Разобьем числа от 0 до $2^n - 1$ на $2^{n-\beta}$ множеств по 2^β элементов в каждом (например, отнеся к i-му множеству числа от $2^\beta i$ до $2^\beta(i+1)$). Чтобы задать любое из этих множеств, нужно задать n, β и число от 0 до $2^{n-\beta}$, указывающее, каким по счету оно является в нашем разбиении. Поэтому энтропия любого из множеств разбиения не превосходит $2\log_2 n + 2\log_2 \beta + (n-\beta) + C$, т.е. $\leq n - \beta + 4\log_2 n + C$ (здесь C – константа, не зависящая от n, α, β.) Если $\alpha + \beta \geq n + 4\log_2 n + C$, то энтропия любого из множеств разбиения не превосходит α, поэтому все числа от 0 до $2^n - 1$ будут (α, β)-стохастическими. (Второе неравенство из определения стохастичности выполнено, т.к. в правой части его стоит $\log_2 2^\beta - \beta = 0$.) Если же $\beta \geq n$, то, взяв в качестве A множество $\{0, 1, \ldots, 2^n - 1\}$, мы убедимся, что его энтропия не превосходит $\log_2 n + C$ (и, следовательно, не превосходит α) и все его элементы являются (α, β)-стохастическими.

б) Пусть α фиксировано. Рассмотрим список $A_1, A_2, \ldots$ $\ldots A_s$ всех конечных множеств, энтропия которых не превосходит α. Очевидно, $s \leq 2^{\alpha+1}$. Мы хотим оценить энтропию семейства $A_1, A_2, \ldots, A_s$. Чтобы задать это семейство, достаточно указать (помимо α) то из описаний множеств $A_1, A_2, \ldots, A_s$, на обработку которого выбранному способу описания

требуется больше всего шагов. Поэтому энтропия указанного семейства не превосходит $\alpha + 2\log_2\alpha + C_1$, где C_1 - некоторая константа, не зависящая от α. Рассмотрим те из множеств $A_1, A_2, \ldots, A_s$, которые имеют менее $2^{n-\alpha-1}$ элементов. Рассмотрим наименьшее число x, не содержащееся в их объединении. Это число меньше 2^n, так как s не превосходит $2^{\alpha+1}$, а каждое из множеств $A_1, \ldots, A_s$ имеет менее $2^{n-\alpha-1}$ элементов.

Чтобы задать число x, нужно указать $A_1, A_2, \ldots, A_s$, α и n, поэтому его энтропия не превосходит

$$\alpha + 2\log_2\alpha + 2\log_2\alpha + 2\log_2 n + C'$$

и тем более $\alpha + 6\log_2 n + C'$ (здесь C' - константа, не зависящая от n и α). Докажем, что если

$$\beta < n - 6\log_2 n - (C'+1) - 2\alpha$$

то построенное нами x не является (α , β)-стохастическим. Из этого будет следовать утверждение теоремы при $C = C'+1$. В самом деле, если x является (α , β)-стохастическим, то $x \in A_i$ и $K(x) \geq \log_2|A_i| - \beta$ при некотором i. Множество A_i должно содержать не менее $2^{n-\alpha-1}$ чисел (иначе x не принадлежало бы ему), поэтому $K(x) \geq n - \alpha - 1 - \beta$.
Но $K(x) \leq \alpha + 6\log_2 n + C'$, откуда $\alpha + 6\log_2 n + C' \geq n - \alpha - 1 - \beta$ и $\beta \geq n - 6\log_2 n - 2\alpha - 1 - C'$. Теорема 2 доказана.

Утверждение теоремы 2 указывает границу для α/n и β/n, при переходе через которую исчезают последние нестохастические объекты. Эта граница (для случая $\alpha = \beta$) находится где-то между I/2 и I/3.

Следующая теорема отвечает на вопрос о доле (α , β)-стохастических чисел среди всех чисел от 0 до $2^n - 1$.

Теорема 3. Существует такое C , что для всех n и для всех α и β , для которых $\alpha \geq C\log_2 n$, количество чисел от 0 до $2^n - 1$, не являющихся (α, β)-стохастическими, заключено между $[2^{n-2\alpha-\beta-C\log_2 n}]$ и $2^{n-\alpha-\beta+C\log_2 n}$, где $[p]$ обозначает целую часть p .

Доказательство. Оценим сначала количество нестохастических чисел сверху. Как и при доказательстве теоремы 2, разобьем множество чисел от 0 до 2^{n-1} на 2^p частей по 2^{n-p} чисел в каждой. Энтропия каждой части не превосходит $p+O(\log_2 n)$, поэтому, выбрав $p=\alpha - C\log_2 n$ при подходящем C , можно добиться, чтобы энтропия любой части не превосходила α . При этом все числа, энтропия которых будет больше $n-p-\beta$ будут (α , β)-стохастическими. Поэтому количество нестохастических чисел не превосходит $2^{n-p-\beta} = 2^{n-\alpha-\beta+C\log_2 n}$. Верхняя оценка получена.

Чтобы получить нижнюю оценку, рассмотрим все множества, энтропия которых не превосходит α , а число элементов не превосходит $2^{n-\alpha-2}$. Энтропия списка всех таких множеств не превосходит $\alpha + O(\log_2 n)$. Объединение всех множеств этого списка содержит не более половины всех чисел от 0 до $2^n - 1$ Через a_i обозначим i-ое (в порядке возрастания) число, не входящее в это объединение (при $i < 2^{n-1}$). В силу сказанного $a_i < 2^n$ при любом $i < 2^{n-1}$. Энтропия a_i не превосходит $\alpha + O(\log_2 n) + O(\log_2 \alpha) + \log_2 i$; (α , β)-стохастическими среди a_i могут быть лишь те, для которых энтропия превосходит $n-2-\alpha-\beta$, т.е. $\alpha + O(\log_2 n) + \log_2 i \geq n-2-\alpha-\beta$ и $\log_2 i \geq n-2\alpha-\beta-O(\log_2 n)$. Поэтому имеется по крайней мере $[2^{n-2\alpha-\beta-O(\log_2 n)}]$ нестохастических чисел. Теорема 3 доказана.

Она показывает, что ("с точностью до $\log_2$") доля (α , β)-стохастических чисел среди всех чисел от 0 до 2^n-1 заключена между $1-1/2^{\alpha+\beta}$ и $1-1/2^{2\alpha+\beta}$.

С точки зрения рассмотренной статистической интерпретации представляет интерес вопрос о том, какова вероятность появления нестохастических чисел в вероятностном эксперименте. Более точно, пусть P - некоторое распределение вероятностей на множестве чисел от 0 до 2^n-1 . Что можно сказать о $P(Q)$, где Q - множество всех нестохастических чисел (при данных α и β)? Естественно желать, чтобы $P(Q)$ было мало. Если не требовать ничего от P , то добиться этого нельзя: P , например, может придавать вероятность 1 некоторому нестохастическому числу. Однако если P имеет малую энтропию, то можно получить желаемую оценку.

Теорема 4. Существует такое C , что для любого распределения вероятностей P, энтропия которого не превосходит α , величина $P(Q)$, где Q - множество всех чисел от 0 до 2^n-1 , не являющихся ($\alpha+C\log_2 n$, β)-стохастическими, не превосходит $2^{-\beta+C\log_2 n}$.

Доказательство. Применяя теорему 1, можно доказывать утверждение с заменой ($\alpha+C\log_2 n$, β)-стохастичности на (α , β)-квазистохастичность. А это делается так. Для всех x , не являющихся (α , β)-квазистохастическими, $K(x)<-\log_2 P(x)-\beta$ или $P(x)<2^{-K(x)-\beta}$. Отсюда

$$2^{\beta}\cdot\sum_{(x\text{ - не }(\alpha,\beta)\text{-квазистохастическое})} P(x) < \sum_{0\le x<2^n} 2^{-K(x)}$$

правая часть не превосходит $n+O(1)$, т.к. количество тех x , для которых $K(x)=a$, не превосходит 2^a.

Литература

I. Агафонов В.Н. Сложность алгоритмов и вычислений. Спецкурс для студентов НГУ, часть 2. Новосибирск: Изд-во НГУ, 1975. 146 с.

2. Вьюгин В.В. Алгоритмическая энтропия (сложность) конечных объектов и ее применение к определению случайности и количества информации. -Семиотика и информатика. М.:ВИНИТИ, 1980, вып. 16, с. 14 - 43.

3. Драгалин А.Г. Математический интуиционизм. Введение в теорию доказательств. М.:Наука, 1979. 256 с.

4. Ершов Ю.Л. Вычислимые функционалы конечных типов. -Алгебра и логика, 1972, т. II, № 4, с. 367 - 437.

5. Звонкин А.К., Левин Л.А. Сложность конечных объектов и обоснование понятий информации и случайности с помощью теории алгоритмов. - Успехи матем. наук, 1970, т. 25, вып. 6 (156), с. 85 - 127.

6. Клини С.К. Введение в метаматематику. Пер. с англ. М.: Изд-во иностр. лит., 1957. 526 с.

7. Колмогоров А.Н. Три подхода к определению понятия "количество информации". - Проблемы передачи информации, 1965, т. I, вып. I, с. 3 - II.

8. Колмогоров А.Н. К логическим основам теории информации и теории вероятностей. - Проблемы передачи информации, 1969, т. 5, вып. 3, с. 3 - 7.

9. Медведев Ю.Т. Финитные задачи. - Докл. АН, 1962, т. 142, № 5, с. 1015 - 1018.

10. Новиков П.С. Конструктивная математическая логика с точки зрения классической. М.:Наука, 1977. 328 с.

11. Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. Пер. с англ. М.:Мир, 1972. 624 с.

12. Успенский В.А., Семенов А.Л. Теория алгоритмов: ее основные открытия и приложения. - В кн.: Алгоритмы в современной математике и ее приложениях. Часть I. / А.П.Ершов, Д.Кнут, редакторы. Новосибирск: Вычислительный центр СО АН СССР, 1982, с. 99 - 342.

13. Шень А. Аксиоматическое описание понятия энтропии конечного объекта. - В кн.: Логика и основания математики. Тезисы VIII Всесоюзной конференции "Логика и методология науки", г. Паланга, 26 - 28 сентября 1982 г. Вильнюс: Вильнюсский университет, 1982, с. 104 - 105.

14. Шень А.Х. Исчисление задач и f_0 -пространства. - В кн.: VI Всесоюзная конференция по математической логике. Тбилиси, 30.XI - 2.XII.1982 г. Тезисы докладов. Тбилиси: Изд-во Тбилисского университета, 1982, с. 204.

15. Шень А.Х. Понятие (α , β)-стохастичности по Колмогорову и его свойства. - Доклады АН, 1983, т. 271, № 6, с. 1337 - 1340.

16. Шень А.Х. Алгоритмические варианты понятия энтропии. - Доклады АН, 1984, т. 276 , № 3 , с. 563 - 566 .

17. Gács P. On the relation between descriptional complexity and algorithmic probability. - Theoretical Computer Science, 1983, v. 22, p. 71 - 93.

18. Kolmogoroff A. Zur Deutung der intuitionistischen Logik. - Mathematische Zeitschrift, 1932, Bd. 35, H. 1, S. 58 - 65.

19. Rose G. F. Propositional calculus and realizability. - Trans. Amer. Math. Soc., 1953, v. 75, p. 1 - 19.

20. Schnorr C. P. Optimal Gödel numberings. - Information Processing, 71. Proceedings of IFIP congress 71 (Lubljana, August, 23 - 28, 1971), v. 1, p. 56 - 58.

21. Schnorr C. P. Optimal enumerations and optimal Gödel numberings. - Mathematical Systems theory, 1975, v. 8, N 2, p. 182 - 191.

Оглавление

Предисловие..2
Введение...3
Глава 1. Понятие f_0 -пространства и его свойства.........14
1.1. Определение f_0 -пространства.................15
1.2. Простейшие примеры f_0-пространств............16
1.3. Полные f_0 -пространства......................18
1.4. Операции над f_0 -пространствами..............23
1.5. Эффективные f_0 -пространства.................33
1.6. Объем на f_0 -пространствах...................40
Глава 2. Задачи и их энтропия..............................41
2.1. Определение задачи. Монотонные и разрешимые задачи...42
2.2. Способы описания. Сложность задачи при данном способе описания..........................43
2.3. Необходимые и достаточные условия для существования оптимального способа описания....44
2.4. Примеры энтропий.................................47
2.5. Сравнение различных энтропий.....................49
2.6. Сравнение энтропий различных задач...............54
Глава 3. Задачи и интуиционистская логика..................55
3.1. Логические операции над задачами.................56
3.2. Энтропия конъюнкции, дизъюнкции и импликации задач..58
3.3. Задачи образуют модель интуиционистского исчисления высказываний.............................63
3.4. Неравенства для энтропии.........................67
3.5. Логика задач.....................................68

Глава 4.

4.I. Различные алгоритмические варианты понятия энтропии как частные случаи нашей схемы............7I

4.2. Неравенства, связывающие различные виды энтропии...8I

4.3. Априорная вероятность и её свойства................85

4.4. Логарифм априорной вероятности и энтропия.........I07

4.5. Аксиоматическое описание энтропии.................II4

4.6. Понятие (α , β)-стохастичности по Колмогорову и его свойства.........................I2I

Список литературы..I29

Оглавление...I32